UPN
UNIVERSIDAD PRIVADA DEL NORTE

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

Carrera de Derecho

"IMPUTACIÓN OBJETIVA EN EL DELITO DE FRAUDE INFORMÁTICO FRENTE A LOS DELITOS CONTRA EL PATRIMONIO EN LIMA, 2024"

Tesis para optar el título profesional de:
Abogada

Autor:

Mirella Astrid Chavez Pascual

Asesor:

Dr. José Manuel Burga Falla
https://orcid.org/0000-0001-5712-2269

Lima - **Perú**

2025

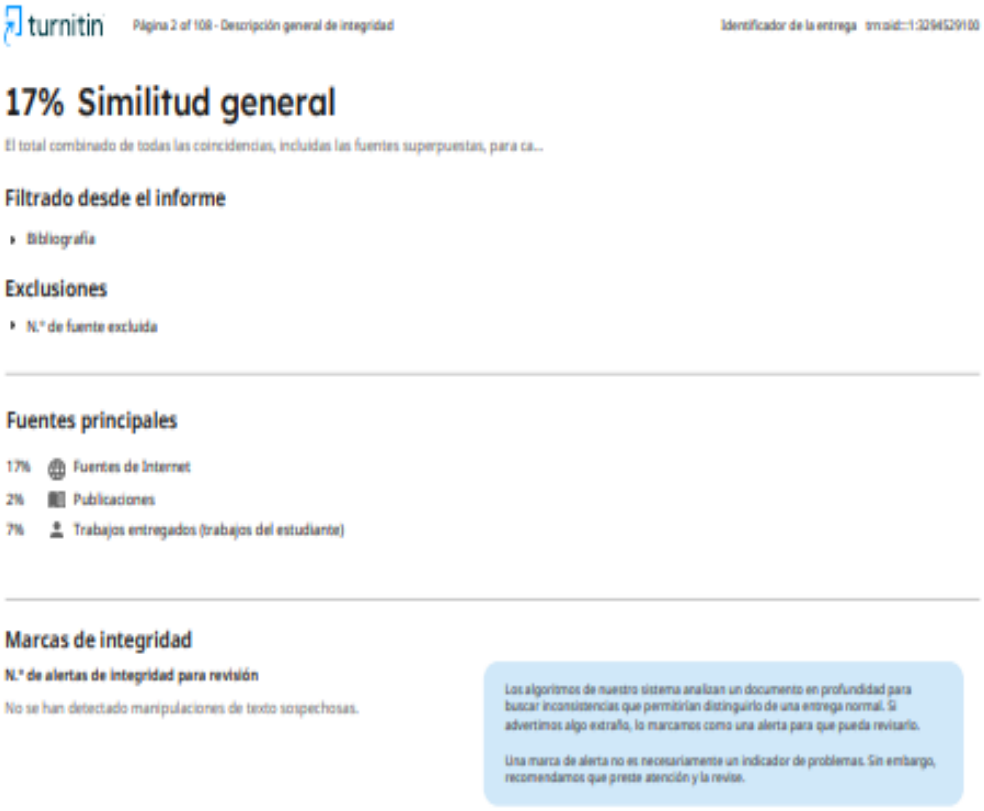
Jurado Evaluador

Jurado 1 Presidente(a)	**JESSIE CATHERINE TAPIA DIAZ**
	Nombre y Apellidos

Jurado 2	**EDWIN ADOLFO MOROCCO COLQUE**
	Nombre y Apellidos

Jurado 3	**JOSE MANUEL BURGA FALLA**
	Nombre y Apellidos

Informe de Similitud



turnitin Página 2 of 108 - Descripción general de integridad Identificador de la entrega trn:oid:::1:3294529100

17% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía

Exclusiones

- N.° de fuente excluida

Fuentes principales

17% Fuentes de Internet
2% Publicaciones
7% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.° de alertas de integridad para revisión

No se han detectado manipulaciones de texto sospechosas.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

Dedicatoria

A mis padres Virna y Medin

Estas líneas son fruto del gran esfuerzo que han hecho para criarme con amor y valores, sus palabras de ánimo me han dado la fortaleza para no rendirme y saber que puedo con todo, su apoyo y amor incondicional no solo me ha demostrado su amor inquebrantable, sino; que no hay obstáculo demasiado grande para creer en mí. Gracias por ser un ejemplo en mi vida y por haber hecho todo lo que está a su alcance para verme feliz, es por ello que esta tesis es tributo al amor infinito y la eterna bondad que me dan, los amo.

Agradecimiento

A mi hermano, por ser la amistad más sincera que conozco, por su paciencia y por ser una persona admirable.

A Fernando, quien me apoya, respalda incondicionalmente y siempre impulsa mis sueños.

A mis estimados docentes les agradezco profundamente la dedicación y paciencia, por acompañarme en este trayecto de aprendizaje.

Índice de Contenido

Índice de tablas

Resumen

La presente investigación analiza la inadecuada imputación del delito de fraude informático y en consecuencia genera confusión con otros delitos como el robo, el hurto y la estafa, es por ello que el objetivo de este proyecto es analizar la aplicación de la imputación objetiva en el delito de fraude informático frente a los delitos contra el patrimonio en Lima. Este proyecto se lleva a cabo mediante un diseño de investigación fenomenológico y descriptivo, con un enfoque cualitativo, asimismo, se recopiló información a través de una entrevista realizada a expertos en la materia, acompañado de instrumentos utilizados como la revisión de casuística y análisis de jurisprudencia. Se espera obtener una comprensión clara de la aplicación de la imputación objetiva en el delito de fraude informático y su distinción de otros delitos, así como identificar áreas de mejora en la legislación y la capacitación. La investigación proporcionará una base sólida para promover la eficacia judicial y la protección de los derechos en casos de delitos informáticos en Lima.

Palabras clave: imputación, fraude informático, robo, hurto, estafa.

Abstract

This research analyzes the inadequate imputation of the crime of computer fraud, which consequently generates confusion with other crimes such as robbery, theft, and fraud. Therefore, the objective of this project is to analyze the application of objective imputation in the crime of computer fraud versus crimes against property in Lima. This project is carried out through a phenomenological and descriptive research design, with a qualitative approach. Information was also collected through interviews with experts in the field, accompanied by instruments such as case study reviews and case law analysis. The aim is to obtain a clear understanding of the application of objective imputation in the crime of computer fraud and its distinction from other crimes, as well as to identify areas for improvement in legislation and training. The research will provide a solid foundation for promoting judicial efficiency and the protection of rights in cases of computer crimes in Lima.

Keywords: imputation, computer fraud, robbery, theft, scam.

CAPÍTULO I. INTRODUCCIÓN

1.1. Contexto problemático

Según el informe de la ONU sobre Ciberdelincuencia Global (2020), el fraude informático ha evolucionado de ser un delito aislado y técnicamente complejo a convertirse en un ecosistema criminal organizado con distintos niveles de especialización y sofisticación.

SEON (2023), señala que algunos países enfrentan una elevada vulnerabilidad ante las ciberamenazas debido a la fragilidad o incluso la ausencia de marcos legales que regulen la ciberdelincuencia. Esta falta de regulación los convierte en zonas de alto riesgo para la seguridad de transacciones sensibles. Entre los diez países peor evaluados en materia de ciberseguridad se encuentran Afganistán, Birmania y Namibia, con puntuaciones respectivas de 5,63, 18,60 y 19,72.

Un avance importante se dio con la Ley N° 30096 (2013), específicamente diseñada para combatir los delitos informáticos, incluyendo el fraude informático en su artículo 8. Esta ley fue posteriormente modificada por la Ley N° 30171 (2014) para alinearla con el Convenio de Budapest sobre Ciberdelincuencia. Como señala el jurista peruano Alfaro: "La evolución normativa peruana en materia de delitos informáticos revela un permanente esfuerzo por adaptar los tipos penales a las nuevas modalidades delictivas que surgen producto del avance tecnológico, aunque con un retraso respecto a la velocidad con que evoluciona la criminalidad informática". Actualmente, la ley vigente es la Ley N° 30096 en su artículo 8 de la Ley N° 30096, definiendo como delito la "alteración, eliminación, supresión o clonación de datos informáticos que induzca a error en la transferencia electrónica de fondos o valores".

A nivel Nacional, conforme los datos del Ministerio Público (2022), los distritos fiscales con mayores ingresos por delitos informáticos fueron en Lima Metropolitana, La

Libertad y Arequipa. En particular, los departamentos de Arequipa y La Libertad con un índice más alto de casos relacionados con delitos informáticos entre los años 2020 y 2023.

Entre los años 2018 y 2021 se evidenció un incremento significativo en las denuncias por ciberdelincuencia. Mientras que en 2018 se registraron 3,031 casos, esta cifra casi se triplicó en 2019 con 7,814 denuncias. En 2020, los reportes ascendieron a 9,787, y en 2021 alcanzaron un total de 12,827, según datos recogidos por la Defensoría del Pueblo. Dentro de los delitos más comunes reportados a la Policía Nacional del Perú destacan el fraude informático y la suplantación de identidad, siendo estos los de mayor recurrencia, junto con otras modalidades delictivas vinculadas al entorno digital.

A nivel nacional, el Ministerio Público informó en 2024 que, durante los dos años anteriores, se recibieron 17,179 denuncias relacionadas con delitos informáticos. De este total, se iniciaron investigaciones preliminares en 10,674 casos, y hasta junio de 2023 se lograron obtener 78 sentencias judiciales.

El presente trabajo expondrá las diferentes investigaciones relacionadas con las categorías investigadas, comenzando con la presentación de los antecedentes internacionales.

Antecedentes investigativos

Antecedentes Internacionales

Paguay (2020), efectuó una investigación orientada a identificar las perspectivas regulatorias concernientes a los delitos informáticos en transacciones comerciales realizadas mediante internet. La población del estudio estuvo constituida por cincuenta y tres profesionales del ámbito jurídico, incluyendo tres magistrados pertenecientes a la Unidad Judicial Penal del Cantón Riobamba. Dada la dimensión reducida de dicha población, no se

requirió la implementación de formulaciones estadísticas para la determinación muestral, procediendo al análisis integral de la totalidad de sujetos. Respecto a la instrumentación metodológica, se implementaron cuestionarios y guías de entrevista. La investigación constató que la LCFE presenta insuficiencias normativas para la adecuada regulación del comercio electrónico, situación que genera un estado de indefensión jurídica para numerosos usuarios. Se identifica como problemática fundamental que dichas operaciones comerciales realizadas a través de medios digitales no se encuentran sometidas a mecanismos de fiscalización por parte de entidades públicas, circunstancia que ha propiciado un incremento en los índices de infracciones vinculadas al comercio electrónico, sin que se vislumbren perspectivas de mitigación. Consecuentemente, se evidencia la necesidad de mayor atención e intervención estatal en materia de regulación del comercio electrónico.

Por otro lado, según Chiluisa (2021), realizó un estudio para identificar las deficiencias jurídicas en el marco ecuatoriano relacionadas con delitos de carácter informático las cuales afectan a la población. Mediante un análisis descriptivo-cualitativo, se examinó la situación actual del país. Los resultados revelan que el uso fraudulento de sistemas informáticos deja desprotegidos a personas naturales y jurídicas debido a vulnerabilidades técnicas. Especialistas informáticos pueden comprometer fácilmente las seguridades de las redes electrónicas, lo que ha logrado un reciente modo de delincuencia organizada que aprovecha la tecnología para obtener beneficios ilícitos. La mayoría de estos delitos quedan impunes por falta de procedimientos preventivos adecuados, situación que demanda acciones urgentes para fortalecer el marco legal y los mecanismos de protección contra el cibercrimen en Ecuador.

El estudio de Cruzado (2021), evalúa el impacto del Convenio de Budapest en el sistema penal argentino, que incorporó nuevas tipificaciones delictivas. La muestra implementada se basa en profesionales expertos en la materia. La investigación utiliza como

instrumento el análisis documental. Las TIC constituyen herramientas fundamentales para el desarrollo socioeconómico en todos los sectores, fortaleciendo una cultura de comunicación indispensable. Este entorno digital diluye las fronteras nacionales debido a la naturaleza virtual de las interacciones, permitiendo que cualquier individuo opere más allá de límites geográficos tradicionales.

Amaya (2024), desarrolló una investigación con el propósito de examinar las implicaciones jurídicas y los retos que enfrenta la persecución de diversos delitos cibernéticos como fraudes y estafas en el ámbito del comercio electrónico colombiano. La metodología empleada se fundamenta en un paradigma interpretativo con enfoque cualitativo, lo cual permitió establecer un análisis del desarrollo normativo en esta materia. Los hallazgos de la investigación revelan una deficiencia significativa en las capacidades institucionales del país. A pesar de las iniciativas implementadas por el gobierno colombiano para fortalecer la ciberseguridad, persiste una insuficiencia en los recursos y competencias necesarios para enfrentar eficazmente las amenazas cibernéticas. Esta situación se manifiesta en respuestas inadecuadas ante incidentes graves, lo que genera una condición de vulnerabilidad tanto para instituciones públicas como para entidades del sector privado.

Según Suárez y Rocafuerte (2024), su investigación busca ejecutar un estudio de semejanzas entre las legislaciones de España, Argentina y Ecuador en materia de delitos informáticos, específicamente en lo concerniente al phishing. Dicho análisis se fundamenta en el estudio doctrinal, considerando los marcos normativos penales de las mencionadas jurisdicciones, así como el Convenio de Budapest, con el objetivo de evaluar las tipificaciones penales en cuanto a la caracterización de la conducta delictiva y las sanciones correspondientes en cada ordenamiento jurídico. La investigación delimitó como objeto de estudio los cuerpos normativos de Argentina, Ecuador y España, realizando un análisis comparado que contempló

dimensiones sociales, históricas y jurídicas relacionadas con el delito informático de phishing. El método usado consistió en examinar la documentación mediante la revisión de su redacción y regulación. El método exegético empleado permitió un análisis pormenorizado de las disposiciones legales, constituyendo un elemento fundamental para la recopilación de información jurídica de las legislaciones estudiadas, observando requisitos y normas gramaticales que contribuyeron a evitar imprecisiones o alteraciones en la investigación, facilitando así una comprensión más clara y accesible para el lector. El estudio determinó que las legislaciones de Ecuador, Argentina y España categorizan el delito de phishing como una modalidad de estafa, lo que establece una convergencia conceptual, mas no normativa. Argentina y España disponen de marcos legales más integrales, plataformas digitales diseñadas para combatir la ciberdelincuencia, y son signatarios del Convenio de Budapest, factores que les permiten mantener una conceptualización precisa de los delitos informáticos. En contraste, Ecuador, a pesar de contar con legislación adecuada, presenta redundancias normativas, dado que existen diversas tipificaciones penales que contemplan conductas similares al phishing, aunque carecen de la especificidad necesaria para abordar comprensivamente esta problemática.

Antecedentes Nacionales

Según Nazario y Villanueva (2022), la investigación tiene como propósito una mejora legislativa para renovar el seguimiento y condena en el delito de fraude informático mediante el modus operandi conocido como phishing. Se abordó por medio de un muestreo no probabilístico, determinado por el investigador, sin el uso de fórmulas específicas. La muestra consistió en 50 participantes de Chiclayo, incluyendo abogados penalistas, jueces y fiscales. La herramienta utilizada para el acopio de datos fue un cuestionario. El análisis reveló que el artículo 8 de la Ley N° 30096, castiga los actos ilícitos cometidos mediante tecnologías

informáticas en perjuicio de una o más personas, imponiendo condenas de hasta ocho años y multas entre sesenta y ciento veinte días. Sin embargo, se identificaron vacíos legales que dejan sin sanción de manera específica la modalidad de phishing.

La investigación de Tuesta (2022), tuvo como objetivo determinar cómo el delito de fraude informático inflige en los derechos fundamentales de los ciudadanos en el distrito de Cercado de Lima durante el año 2022. Para ello, utilizaron una muestra con expertos en el área y se emplearon técnicas de recopilación de datos y análisis documental. Obteniendo como resultado que el fraude informático impacta considerablemente en los derechos fundamentales, demostrando que infringe derechos específicos, así como principios y garantías esenciales para las personas.

Valdivia (2023), buscó valorar la efectividad de las herramientas empleadas en el seguimiento penal del fraude informático en Perú. La muestra del estudio comprendió estadísticas de denuncias por delitos de fraude informático en fiscalías de Lima Norte y Lima Centro (en proceso, archivadas y formalizadas), encuestas a 26 participantes entre profesionales del derecho, autoridades y ciudadanos, y entrevistas a 15 expertos del ámbito jurídico. Para la acumulación de cifras se implementaron análisis documentales: fichas bibliográficas y de resumen, encuestas, entrevistas y análisis estadísticos. El estudio concluyó que las técnicas investigativas empleadas por la Fiscalía se categorizan en: (1) actuaciones comunes como declaraciones y pericias; (2) actuaciones jurisdiccionales que requieren autorización judicial, incluyendo levantamiento del secreto de comunicaciones, acceso a información bancaria, allanamientos y geolocalización, permitiendo identificar a titulares de líneas telefónicas y cuentas bancarias, así como incautar elementos relacionados con el delito; (3) técnicas especiales como el agente encubierto, que facilita la identificación de miembros y líderes de organizaciones criminales; y (4) cooperación internacional con proveedores de

internet como Google, Microsoft o Netflix para obtener información de suscriptores que pudieran estar vinculados a actividades ilícitas.

Según Chuco (2023), la intención fundamental de su trabajo fue examinar la vinculación entre el delito de fraude informático y el hurto como delito precedente, en el contexto del Cercado de Lima durante el año 2020. El estudio se realizó con una muestra constituida por seis juristas especializados en la materia. El método empleado para la recolección de datos se fundamentó en la aplicación de guías de entrevista. La investigación concluyó que el delito de fraude informático no debe ser subsumido dentro de las modalidades específicas del hurto como delito previo, ni debe considerarse dependiente o subordinado a un delito base, rechazando la premisa de que su configuración esté condicionada a la consumación previa del delito de hurto. Adicionalmente, se enfatiza la necesidad de un análisis meticuloso en cada denuncia para determinar adecuadamente la modalidad y circunstancias fácticas. El estudio señala que, inicialmente, en el ordenamiento jurídico-penal, el fraude informático fue tipificado como una circunstancia agravante del delito de hurto. No obstante, surgieron posiciones doctrinales que abogan por una regulación autónoma del fraude informático, en atención a sus características operativas particulares, sosteniendo que no debería configurarse como dependiente de un delito base ni considerarse que su materialización estuviera condicionada a la consumación previa del delito de hurto.

Condori (2020), baso su trabajo en identificar las implicaciones jurídicas del fraude informático y su vínculo con la protección penal en delitos contra el patrimonio en el Distrito Fiscal de Lima Norte. La búsqueda se centró en los funcionarios de dicho distrito fiscal como población. Para el acopio de datos, se usó: guía de entrevistas con 8 preguntas abiertas, diseñadas de acuerdo con las categorías y subcategorías definidas; una guía de observación para registrar información durante las entrevistas en su contexto natural; y una guía de análisis

documental para comparar la información obtenida de las fuentes bibliográficas con las respuestas de las entrevistas. El estudio concluyó que el fraude informático vinculado a delitos patrimoniales implica conductas que coinciden con otras tipificaciones de delitos patrimoniales. Aunque el fraude informático se refiere a causar un daño patrimonial mediante la modificación o manipulación de datos y software en sistemas informáticos, la investigación señaló que, a pesar de su relevancia actual, aún existe una falta de claridad metodológica que dificulta la realización de investigaciones efectivas para obtener resultados satisfactorios en estos casos.

Según Mancilla (2022), el objetivo de este estudio fue observar el empleo de la acusación fiscal en casos de fraude informático en el Distrito Fiscal de Lima durante el año 2022. La muestra estuvo conformada por 51 miembros de la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima Centro, 100 efectivos policiales de la división de investigación de delitos de alta tecnología y 30 abogados especialistas. Se uso la encuesta como técnica de recolección de datos y se empleó un cuestionario estructurado como instrumento. Los resultados mostraron una aplicación inadecuada de la acusación fiscal en los casos de fraude informático en el Distrito Fiscal de Lima en 2022. La problemática se basa en dos factores principales: en primer lugar, la incorrecta tipificación de los delitos de fraude electrónico, que dificulta que los fiscales formulen acusaciones técnicamente adecuadas; y en segundo lugar, la constante evolución de los sistemas digitales, que genera una innovación continua en las modalidades delictivas electrónicas, lo que hace que la normativa peruana sea insuficiente para abordar de manera efectiva estos nuevos retos.

La investigación de García (2023), se propuso examinar la relación entre la obtención fraudulenta de créditos bancarios durante la pandemia de COVID-19 y el delito informático, bajo el marco legal vigente en 2021. La muestra se basó en profesionales expertos en la materia.

El estudio empleó metodología cualitativa con muestreo no probabilístico, fundamentado en criterios subjetivos en vez de selección aleatoria. Este enfoque por cuotas permitió identificar el perfil que predisponen a individuos a perpetrar fraudes crediticios bancarios mediante medios informáticos. Se realizo una guía de entrevista para la recolección de datos. La investigación concluyó que el fraude crediticio bancario carece de tipificación específica en el código penal peruano. Si bien existen normativas asociadas, como aquellas referentes a delitos contra el orden financiero y la Ley 30096 de Delitos Informáticos, estas no contemplan claramente disposiciones específicas para esta modalidad de ciberdelito, especialmente en el contexto pandémico. Consecuentemente, el estudio propone la conveniencia de desarrollar un anteproyecto legislativo que incorpore explícitamente este delito en el código penal.

Bases teóricas

En el presente estudio se abordará en profundidad las categorías y subcategorías vinculadas a la imputación objetiva en el delito de fraude informático, así como su relación con los delitos contra el patrimonio en la ciudad de Lima, durante el periodo comprendido entre 2019 y 2024. Desde una perspectiva jurídico-social, se analizarán los elementos normativos, doctrinarios y prácticos que permiten comprender el tratamiento de estas conductas delictivas en el marco del sistema penal peruano.

La primera categoría se centra en la imputación objetiva en el delito de fraude informático, abordando como subcategorías tanto los elementos constitutivos del fraude informático como la aplicación concreta del principio de imputación objetiva en estos casos. Para ello, se utilizarán como instrumentos metodológicos la guía de entrevista a operadores del sistema de justicia penal (jueces y abogados) y el análisis documental de casos y sentencias. Este apartado busca determinar cómo se configura la responsabilidad penal del autor en delitos

que involucran medios tecnológicos, y cómo se ha interpretado la relación de causalidad y el riesgo jurídicamente desaprobado en el marco de estos ilícitos.

La segunda categoría se refiere a los delitos contra el patrimonio en Lima durante el año 2024, con un enfoque comparativo que incluye la descripción de los delitos de robo, hurto y estafa, considerados como los más frecuentes y representativos de afectación patrimonial en el contexto urbano. Estas subcategorías serán abordadas también mediante entrevistas a expertos y análisis documental, con el propósito de identificar cómo estas figuras tradicionales delictivas se diferencian o se solapan con nuevas formas de criminalidad, como el fraude informático.

Este análisis teórico busca no solo establecer las bases conceptuales y legales del tema, sino también proporcionar un panorama integral sobre cómo la transformación digital y el desarrollo de nuevas modalidades delictivas están desafiando las estructuras tradicionales del derecho penal y exigiendo nuevas formas de interpretación y aplicación normativa en el contexto peruano actual.

Definición de Delito

Un delito es una acción que viola lo dispuesto por la ley y que requiere una sanción o pena conforme a la normativa legal. Según Carrara, el delito puede definirse como el incumplimiento de las normas legales impuestas por el Estado con el propósito de salvaguardar el bienestar ciudadano. Esta transgresión se manifiesta a través de comportamientos concretos realizados por las personas, ya sean acciones u omisiones, que resultan reprochables desde una perspectiva ética y perjudiciales para la sociedad en su dimensión política. La determinación de qué conductas constituyen delito evoluciona con la sociedad misma, reflejando los valores

y principios que cada comunidad considera fundamentales para su coexistencia pacífica y desarrollo.

Delitos Informáticos

El artículo primero de la Ley N.º 30096, conocida como la Ley de Delitos Informáticos, señala que su finalidad principal es prevenir y sancionar conductas ilícitas que afecten negativamente a los sistemas y datos informáticos, así como a otros bienes jurídicos protegidos penalmente, cuando estas acciones se cometen mediante tecnologías de la información o comunicación. El propósito es garantizar una respuesta efectiva frente a la ciberdelincuencia.

Por su parte, Téllez Valdés (2003) advierte que los ataques contra sistemas de información constituyen una amenaza significativa para el desarrollo de una sociedad digital más segura, así como para la consolidación de un entorno basado en la libertad, la seguridad y la justicia. Esto resalta la necesidad de abordar este fenómeno con total seriedad.

Definición de Fraude Informático

El concepto de fraude informático hace referencia a situaciones en las que una persona obtiene, para sí misma o para un tercero, un beneficio indebido mediante la manipulación, alteración o interferencia en un sistema informático. En otras palabras, este delito se configura cuando se utiliza la tecnología de manera ilícita para afectar sistemas digitales con el fin de obtener un provecho, generalmente en perjuicio de otro.

Modalidades de Fraude informático

Definición de Phishing

Según Oxman (2013), el "phishing" es un tipo de fraude informático cuyo objetivo principal es obtener información personal de un usuario de Internet, con el fin de acceder a sus cuentas de correo electrónico o redes sociales y, además, obtener datos de sus contactos virtuales para comercializarlos ilegalmente. También se busca conseguir claves de "e-banking" para ingresar a las cuentas bancarias de las víctimas y robar el dinero mediante transferencias a un tercero conocido como "mulero".

Según Vargas (2020), los "muleros" actúan como intermediarios entre los delincuentes y las víctimas del phishing. Estos muleros son reclutados a través de ofertas de trabajo falsas, que aparecen en portales nacionales, canales de mensajería instantánea o incluso en correos no solicitados. Otro tipo común de fraude en los últimos años es el "phishing car", que consiste en anuncios de automóviles, generalmente de alta gama, a precios muy bajos. Una vez pagado el precio, el vendedor desaparece sin entregar el vehículo.

De la misma forma, los ataques se llevan a cabo empleando técnicas de ingeniería social, que crean un entorno de manipulación psicológica con el objetivo de engañar a usuarios o empleados para que entreguen sus credenciales de acceso u otra información confidencial. Con frecuencia, se utiliza el correo electrónico u otros medios de comunicación que generan urgencia, miedo o emociones similares en la víctima, lo que la lleva a revelar rápidamente información sensible, hacer clic en un enlace malicioso o abrir un archivo comprometido (Hadnagy, 2011).

Definición de Vishing

Otra forma de estafa que ha impactado repetidamente a los usuarios es el **vishing**, una técnica de fraude telefónico en la que los estafadores contactan a la víctima para manipularla y obtener datos sensibles, como información personal, financiera o de seguridad. En algunos casos, incluso logran convencer a la persona de realizar transferencias de dinero (Europol, 2020).

Una de las formas en que operan los ciberdelincuentes es mediante la suplantación de llamadas telefónicas de falsas instituciones bancarias. Utilizando un engaño y replicando de manera exacta la voz de la entidad financiera, se comunican con los clientes y mencionan un cargo no reconocido. Al obtener el nombre completo y algunos números relacionados con las tarjetas, los delincuentes logran generar inquietud y preocupación en las víctimas, y aprovechando el factor sorpresa, llevan a cabo una falsa cancelación de la transacción (Vargas, 2020).

Definición de Smishing

Según INCIBE (2024), El smishing es un método de ciberataque donde los delincuentes envían mensajes SMS haciéndose pasar por organizaciones legítimas como bancos, instituciones gubernamentales o redes sociales. Su propósito es obtener información confidencial de las víctimas o conseguir beneficios económicos fraudulentos. Estos mensajes suelen contener señuelos para que el receptor realice alguna acción perjudicial, como llamar a números telefónicos con costos elevados o hacer clic en enlaces que conducen a sitios web fraudulentos. Los pretextos utilizados varían, pero siempre buscan manipular al usuario para que revele datos personales o realice pagos no deseados.

Estándares de Imputación

Los estándares de imputación constituyen el marco normativo y jurisprudencial que determina cuándo y cómo puede atribuirse responsabilidad penal a un sujeto por la comisión de un hecho delictivo. Estos criterios establecen con precisión los elementos que deben concurrir para que legalmente pueda considerarse a una persona como responsable de un acto punible.

Definición de imputación subjetiva

La imputación subjetiva se centra en el aspecto interno del comportamiento delictivo, evaluando el estado mental del autor al momento de la comisión del delito. Esta dimensión examina: El dolo se refiere al conocimiento y la intención de llevar a cabo los elementos objetivos del tipo penal, mientras que la culpa implica la violación del deber de cuidado que se requiere. Además, existen diferentes niveles de intencionalidad que pueden influir en la responsabilidad penal, así como la capacidad del autor para prever el resultado de sus acciones.

Puig (2016), refiere que la imputación subjetiva se refiere a la verificación de que la conducta que objetivamente aparece como típica haya sido cometida con dolo o culpa, es decir, con alguna de las formas de vinculación subjetiva previstas en la ley.

Definición de imputación objetiva

La imputación objetiva examina la conexión entre la conducta y el resultado desde un enfoque normativo, trascendiendo la simple causalidad física. Sus elementos clave son: la generación de un riesgo que el ordenamiento jurídico desaprueba, la realización de ese riesgo

en el resultado ocurrido, la evaluación de si el resultado está dentro del alcance de protección de la norma, y la comprobación del vínculo causal entre la acción u omisión y el daño causado.

Roxin (1997), señala que la teoría de la imputación objetiva intenta determinar, con criterios normativos, las propiedades objetivas generales que debe presentar un comportamiento para que pueda ser prohibido por una norma jurídico-penal bajo amenaza de pena. Esta teoría permite excluir la responsabilidad en casos donde, pese a existir causalidad natural, no puede atribuirse normativamente el resultado al autor por ausencia de alguno de estos requisitos.

Delitos contra el Patrimonio

Los delitos contra el patrimonio son aquellos actos ilegales que impactan los bienes materiales o recursos económicos de una persona o entidad. Estos delitos abarcan robos, hurtos, estafas, fraudes y cualquier otra acción que implique la apropiación o daño de los bienes o recursos financieros de una persona o entidad.

Definición de Robo

El robo es un delito contra el patrimonio que consiste en la apropiación ilegal de bienes o propiedades ajenas, con la intención de obtener un beneficio económico para uno mismo o para otro, sin el consentimiento del propietario. Este delito se distingue por la apropiación indebida de bienes de otra persona, con el objetivo de obtener un beneficio económico, sin la autorización del dueño.

Según Conde (2019), el robo se diferencia del hurto por el uso de violencia o intimidación hacia las personas, o de fuerza sobre los objetos. Estos elementos incrementan la

gravedad del delito y justifican una sanción más severa. No solo se ve afectado el patrimonio, sino que también se pone en riesgo otros bienes jurídicos, como la integridad física o la libertad.

Definición de Hurto

El hurto es un delito contra el patrimonio que implica la apropiación de bienes muebles de otra persona sin recurrir a la violencia o intimidación directa sobre la víctima, con el fin de obtener un beneficio personal o para otro. En otras palabras, se trata de la toma ilegítima de bienes muebles sin emplear violencia ni amenazas hacia la persona ni causar daño a los objetos.

Zaffaroni (2007) señala que el hurto es el delito principal dentro de los delitos contra el patrimonio. Consiste en apoderarse de un bien mueble ajeno de manera ilegal, sin emplear violencia o amenazas contra las personas ni dañar los bienes.

Definición de Estafa

La estafa es un delito en el que una persona manipula a otra para obtener un beneficio económico o material, induciéndola a realizar un acto que resulte en un perjuicio económico o patrimonial para la víctima. Esto puede implicar el uso de mentiras, artificios o engaños con el propósito de obtener bienes, dinero o servicios de manera fraudulenta. Se configura cuando alguien engaña a otra persona para conseguir un beneficio económico o material, llevándola a tomar decisiones que ocasionen daño patrimonial, mediante el uso de falsedades o trucos.

Ripollés (2013), la estafa se comete cuando, a través de engaños, trucos, artimañas u otros métodos fraudulentos para inducir al error, se logra que la víctima, sin conocer la verdad, realice una acción que perjudica su patrimonio o el de otro. Este delito implica una secuencia de engaño, error, disposición patrimonial y perjuicio.

Justificación

Justificación teórica

La presente investigación posee una justificación teórica sólida, ya que busca analizar cómo se aplica la imputación objetiva en el delito de fraude informático en comparación con los delitos contra el patrimonio en Lima. Este análisis permitirá comprender las interpretaciones doctrinarias y prácticas jurídicas predominantes en el sistema penal peruano.

Justificación práctica

Desde una perspectiva práctica, esta estudio se justifica por la necesidad urgente de abordar el incremento de casos de fraude informático en Lima, los cuales tienen un impacto negativo directo en la seguridad digital, la economía y la confianza ciudadana. Este tipo de ciberdelitos afecta tanto a individuos como a empresas, exponiendo vacíos normativos y desafíos en la persecución penal. Por ello, estudiar cómo se está aplicando el principio de imputación objetiva en estos casos resulta crucial para mejorar la respuesta del sistema judicial, reducir los niveles de impunidad y ofrecer a las víctimas herramientas jurídicas más eficaces para enfrentar estas situaciones. El análisis también busca contribuir a una futura propuesta de regulación penal más adecuada al contexto digital contemporáneo.

Justificación metodológica

La justificación metodológica se sustenta en el enfoque cualitativo adoptado para esta investigación. A través de la recolección e interpretación de información mediante entrevistas y análisis documental, se busca obtener datos contextualizados y fundamentados en la realidad actual. Este enfoque permitirá examinar las prácticas jurídicas y las percepciones de los operadores del derecho en torno al fraude informático y los delitos patrimoniales,

proporcionando una visión integral y actualizada del problema. Esta metodología es pertinente para abordar una problemática compleja, en la que convergen aspectos legales, tecnológicos y sociales, y resulta especialmente útil para generar propuestas que contribuyan a la prevención y mitigación de los delitos informáticos.

1.2. Formulación del problema

Problema general

P.G. ¿Cómo se aplica la imputación objetiva en el delito de fraude informático frente a los delitos contra el patrimonio en Lima, 2024?

Problemas específicos

PE1. ¿Cuáles son las principales dificultades que enfrenta los procedimientos por robo al aplicar la imputación objetiva en los casos de fraude informático?

PE2. ¿Cuáles son las principales dificultades que enfrenta los procedimientos por hurto al aplicar la imputación objetiva en los casos de fraude informático?

PE3. ¿Cuáles son las principales dificultades que enfrenta los procedimientos por estafa al aplicar la imputación objetiva en los casos de fraude informático?

1.3. Objetivos

Objetivo general

O.G. Analizar la aplicación de la imputación objetiva en el delito de fraude informático frente a los delitos contra el patrimonio en Lima, 2024.

Objetivos específicos

OE1: Identificar las principales dificultades que enfrenta los procedimientos por robo al aplicar la imputación objetiva en los casos de fraude informático.

OE2: Identificar las principales dificultades que enfrenta los procedimientos por hurto al aplicar la imputación objetiva en los casos de fraude informático.

OE3: Identificar las principales dificultades que enfrenta los procedimientos por estafa al aplicar la imputación objetiva en los casos de fraude informático.

CAPÍTULO II. METODOLOGÍA

2.1. Enfoque del estudio

El presente estudio adopta un enfoque cualitativo, ya que busca comprender y examinar cómo se está aplicando la imputación del delito de fraude informático en relación con los delitos contra el patrimonio. De acuerdo con Maldonado (2018), la investigación cualitativa se distingue por emplear múltiples métodos y por analizar los fenómenos en su contexto natural, interpretándolos desde una perspectiva comprensiva y contextual.

2.2. Nivel de investigación

La investigación se enmarca en el nivel descriptivo, lo que implicó la recopilación de fuentes casuísticas y jurisprudenciales. Además, se llevaron a cabo entrevistas con expertos en el área, incluyendo magistrados de los Juzgados de Investigación Preparatoria de Lima Norte y especialistas judiciales. Del mismo modo, se trata de una investigación de carácter básico, ya que se enfoca en el análisis de conceptos doctrinarios con el propósito de aportar al entendimiento de la problemática y alcanzar los objetivos planteados.

2.3. Diseño de investigación

El diseño de la investigación tiene un enfoque fenomenológico. Según Husserl (1992), la fenomenología presenta un método descriptivo innovador y una ciencia apriorística derivada de ella, que está destinada a proporcionar la base esencial para una filosofía científicamente rigurosa.

2.4. Participantes

La correcta elección del objeto de estudio y la delimitación precisa del problema de investigación son aspectos esenciales para garantizar los recursos adecuados que permitan desarrollar el estudio con éxito. De acuerdo con Mejía (2005), la población se entiende como

el conjunto de personas que comparten características similares y cumplen con ciertos criterios establecidos, lo cual permite determinar cuántos participantes formarán parte de la investigación.

En este caso, se identificó como población a un conjunto específico de jueces y abogados especializados en el tema perteneciente a la Corte Superior de Justicia de Lima Norte.

Participantes:

1. Mg. Wilmer Roy Quispe Umasi
2. Mg. Cynthia Celeste Gálvez Marín
3. Mg. Rocio Robles Ramos
4. Abg. Evelin Nelsi Durand Melgarejo
5. Abg. Dannesa Alicia Fernández Calderón

2.5. Muestra

Tabla 1

Casuística sobre fraude informático en el Perú.

N.º	Caso	Institución Judicial	Sentenciado/a
1	Condena anticipada por fraude informático (Caso Úrsula Durand Valdez)	Primer Despacho de la Fiscalía Especializada en Ciberdelincuencia de Lima Centro	Úrsula Durand Valdez
2	Sentencia por fraude informático en el Metro de Lima (Caso José Félix Primera Santana)	Corte Superior de Justicia de Lima Sur, Tercer Juzgado de Investigación Preparatoria	José Félix Primera Santana
3	Primer caso de fraude informático con criptomonedas (Caso José Leonell Llanos Rodríguez)	Fiscalía Especializada en Ciberdelincuencia de Lima Centro	José Leonell Llanos Rodríguez

Nota. Elaboración propia basada en fuentes judiciales obtenidas a través de portales del Poder Judicial y la Fiscalía Especializada en Ciberdelincuencia (2022–2024).

Tabla 2

Resumen de Jurisprudencia Constitucional y de Casación sobre Fraude Informático en el Perú.

N.º	Fuente	Institución	Sentenciado/a
1	STC Exp. 01189-2019-PHC/TC	Tribunal Constitucional del Perú	Marcos Morales Vargas
2	Casación N.º 536-2020 / Arequipa	Corte Suprema de Justicia de la República	Roberto Víctor Salas Vilca
3	Casación N.º 3330-2022 / El Santa	Corte Suprema de Justicia – Sala Penal Permanente	Marco André Gómez García
4	Casación N.º 2872-2022 / San Martín	Corte Suprema de Justicia – Sala Penal Permanente	No se especifica el nombre

Nota. Elaboración propia con base en jurisprudencia constitucional y casatoria del Tribunal Constitucional y la Corte Suprema del Perú (2020–2024).

Tabla 3

Lista de Entrevistados.

N.º	Expertos	Años de Experiencia	Función
1	Mg. Wilmer Roy Quispe Umasi	11 años	Juez del 9no Juzgado del JIP
2	Mg. Cynthia Celeste Gálvez Marín	13 años y 11 meses	Jueza del 6to Juzgado del JIP
3	Mg. Rocio Robles Ramos	10 años	Jueza del 5to Juzgado del JIP
4	Abg. Evelin Nelsi Durand Melgarejo	03 años	Especialista Judicial
5	Abg. Dannesa Alicia Fernández Calderón	04 años con 5 meses	Especialista Judicial

Nota. Elaboración propia sobre los años de experiencia de la vida profesional de los entrevistados.

2.6. Técnicas e Instrumentos y análisis de datos

El presente estudio se desarrolló bajo un enfoque cualitativo, orientado a la comprensión profunda del fenómeno jurídico de la imputación objetiva en el contexto del fraude informático, en contraste con los delitos patrimoniales tradicionales. Para ello, se emplearon tres técnicas centrales: el análisis casuístico, la revisión jurisprudencial y las entrevistas a expertos. Estas herramientas permitieron abordar el problema desde un enfoque interpretativo, contextual y crítico, garantizando una mirada integral del objeto de estudio.

Análisis documental

El análisis casuístico se basó en la revisión sistemática de casuísticas relevantes emitidas por órganos jurisdiccionales. En particular, se analizaron casos del Ministerio Público y del Poder Judicial que abordaron sucesos concretos de fraude informático. Este instrumento permitió identificar cómo el sistema penal sanciona conductas que afectan la seguridad de los medios de pago electrónicos. A través de este tipo de documentos, se examinó no solo la aplicación concreta de la Ley N.º 30096, sino también la relevancia de las pruebas digitales, la reparación civil y las medidas preventivas adoptadas, necesario para comprender el tratamiento jurídico del fraude informático en el Perú, así como su diferenciación respecto de otros delitos contra el patrimonio.

El análisis jurisprudencial se aplicó a través del estudio detallado de resoluciones de tribunales ordinarios (como sentencias de primera y segunda instancia y recursos de casación), como también decisiones del Tribunal Constitucional, a fin de identificar criterios relevantes sobre la tipificación, sanción y aspectos procesales del fraude informático. Las sentencias seleccionadas permitieron observar cómo los jueces interpretan y aplican las normas en casos concretos, destacando elementos como la valoración de pruebas digitales, la procedencia de

penas alternativas, y el respeto a principios constitucionales como la legalidad, el debido proceso y la tutela jurisdiccional efectiva, con el objetivo de comprender cómo se aplican los estándares legales en la práctica.

Para minimizar sesgos en este análisis documental, se aplicaron criterios claros y objetivos en la selección de documentos y casos, evitando interpretaciones sesgadas y manteniendo un enfoque imparcial en el análisis de la información disponible. En conjunto, estos métodos de recolección de datos fueron fundamentales para obtener una comprensión profunda y rigurosa de la aplicación de la imputación objetiva en el delito de fraude informático frente a los delitos contra el patrimonio en lima, asegurando la validez y la objetividad en la investigación realizada.

Guía de Entrevista

La técnica utilizada en el estudio fue la entrevista individual. De acuerdo con Díaz (2013), la entrevista es un método que facilita la comunicación interpersonal entre uno o más participantes, con el objetivo de obtener información sobre sus opiniones o criterios respecto al tema de investigación, a través de una conversación dirigida hacia una finalidad específica.

En ese sentido, se llevó a cabo las entrevistas con jueces y abogados especializados, quienes aportaron valiosas perspectivas sobre los desafíos que enfrenta el sistema judicial y las mejoras necesarias en la imputación del delito de fraude informático. Estas entrevistas fueron fundamentales para identificar las dificultades en la aplicación de la ley y las posibles soluciones que podrían fortalecer la persecución de este tipo de delitos.

2.7. Procedimiento de recolección de datos

Los datos recolectados fueron organizados en matrices temáticas, que facilitaron la clasificación de la información conforme a las categorías y subcategorías previamente establecidas en el marco teórico. Entre las principales categorías analizadas se encuentran: la imputación objetiva en el delito de fraude informático lo que englobo las definiciones del delito, el fraude informático, modalidades del delito de fraude informático, la imputación objetiva y subjetiva y como segunda categoría se tiene los delitos contra el patrimonio como robo, hurto y estafa en lima, incluyendo percepciones doctrinales y judiciales extraídas de las entrevistas.

El análisis documental consistió en una revisión sistemática de casos judiciales relevantes, seleccionados a partir de sentencias emitidas por el Poder Judicial del Perú. Esta técnica permitió examinar cómo se resuelven concretamente casos de fraude informático, identificando patrones en la calificación jurídica, la argumentación judicial sobre la imputación objetiva y el tratamiento diferenciado respecto de los delitos patrimoniales clásicos. Se prestó especial atención a los elementos probatorios utilizados, la argumentación sobre la creación de riesgo jurídicamente desaprobado y la atribución de responsabilidad penal en contextos mediados por sistemas tecnológicos.

En cuanto al análisis jurisprudencial, se examinó un conjunto significativo de sentencias emitidas por órganos jurisdiccionales. Este análisis permitió observar cómo los tribunales justifican la atribución objetiva del resultado lesivo cuando la conducta punible se produce a través de sistemas informáticos. Se prestó especial atención a elementos como la previsibilidad del daño, la creación de riesgos jurídicamente desaprobados, la causalidad normativa y la interpretación de los tipos penales en contextos tecnológicos complejos.

De forma complementaria, se realizaron entrevistas semiestructuradas a jueces penales y académicos con experiencia en el campo. Las entrevistas fueron transcritas, y categorizadas temáticamente. Este insumo cualitativo resultó fundamental para contrastar la doctrina con la práctica judicial, identificar vacíos normativos y conocer las principales dificultades probatorias y dogmáticas que enfrentan los operadores jurídicos frente a delitos informáticos. Además, las entrevistas permitieron captar percepciones sobre la aplicación de la imputación objetiva como criterio de atribución penal en este tipo de casos.

2.8. Aspectos éticos

Se ha respetado en todo momento los derechos de autor y se han seguido los principios éticos fundamentales para la realización de esta investigación. Todos los participantes brindaron su consentimiento informado tras recibir una explicación clara y accesible sobre los objetivos del estudio, el manejo confidencial de sus datos y el uso previsto de los resultados. En cuanto a la credibilidad de la investigación, se ha garantizado una presentación precisa y objetiva de los hechos y hallazgos, reflejando fielmente la problemática social abordada. Asimismo, se ha manejado con especial cuidado toda la información recopilada, citando correctamente las fuentes conforme al estilo APA establecido por la Universidad Privada del Norte. Se han cumplido todos los procedimientos y normativas requeridas por la universidad para la aprobación de la tesis, con un enfoque orientado a generar un impacto social positivo. Cabe resaltar que toda la información utilizada proviene de fuentes fidedignas, lo cual respalda la transparencia e integridad del estudio.

CAPÍTULO III. RESULTADOS

3.1. Resultados de análisis documental

Análisis casuístico de sentencias por fraude informático

En relación con el Objetivo General

Caso "Sentencia a extranjero por el delito de fraude informático"

FUENTE DOCUMENTAL	CONTENIDO DE LA FUENTE DOCUMENTAL	ANÁLISIS DEL CONTENIDO DE LA FUENTE DOCUMENTAL	CONCLUSIÓN
Institución: Corte Superior de Justicia de Lima Sur, Tercer Juzgado de Investigación Preparatoria Caso: Sentencia por fraude informático en el Metro de Lima Sentenciado: José Félix Primera Santana Agraviado: Ministerio de Transportes y Comunicaciones	José Félix Primera Santana recibió una condena por alterar tarjetas del Tren Eléctrico de Lima con el fin de facilitar el ingreso de personas a cambio de dinero. La Corte Superior de Justicia de Lima Sur dictó una sentencia de dos años y medio de prisión suspendida y ordenó el pago de mil soles como reparación civil al Ministerio de Transportes y Comunicaciones.	**Modalidad del Fraude:** José Félix Primera Santana alteraba tarjetas del Tren Eléctrico con el propósito de facilitar el ingreso indebido de personas a cambio de dinero. Esta modalidad evidencia las debilidades tecnológicas del sistema de transporte frente a posibles manipulaciones. **Sentencia y Consecuencias Legales:** La condena de dos años y seis meses de prisión suspendida refleja la firme postura del sistema judicial peruano frente a los delitos informáticos. Asimismo, la imposición de una reparación civil de mil soles destaca la responsabilidad económica del infractor y la necesidad de resarcir al Ministerio de Transportes y Comunicaciones, entidad afectada por el delito. **Importancia y Contexto:** Este caso representa uno de los primeros en su tipo en el país, subrayando la creciente incidencia de delitos informáticos en la sociedad actual. La celeridad con la que se dictó la sentencia, en tan solo un día, demuestra el compromiso del Poder Judicial con la protección del transporte público y la seguridad ciudadana. **Avances en Justicia Digital:** La Corte Superior de Lima Sur reafirma su compromiso con una justicia eficaz, especialmente en situaciones que comprometen la integridad digital y la seguridad pública. Este caso podría establecer un precedente importante y actuar como medida disuasoria ante futuros delitos informáticos en el ámbito del transporte.	El caso de José Félix Primera Santana y su condena por fraude informático en el Metro de Lima subraya la importancia de la seguridad tecnológica en el transporte público y la respuesta efectiva del sistema judicial ante tales delitos. La sentencia refleja la gravedad del fraude informático y el compromiso de las autoridades peruanas con la protección de la función y seguridad pública en la era digital.

Nota. Elaboración propia.

Interpretación:

El caso de José Félix Primera Santana revela cómo los delitos de fraude informático pueden perpetrarse mediante acciones relativamente simples, pero con un alto impacto en bienes públicos. La manipulación de tarjetas del Tren Eléctrico de Lima para facilitar el ingreso de personas no autorizadas, a cambio de dinero, constituye una afectación directa al patrimonio del Estado y a la seguridad del sistema de transporte.

Desde el panorama, como de la imputación objetiva, el hecho ilícito atribuido a Primera Santana cumple con los componentes suficientes para ponderar su actuación como penalmente relevante: existe una creación de un riesgo no permitido la adulteración tecnológica que se concreta en un resultado dañoso para una institución estatal. Además, este resultado es previsible y evitable por parte del autor, lo que justifica la atribución jurídica del resultado conforme a los criterios de esta teoría.

La sentencia impuesta, que incluye una pena suspendida y una reparación civil, refleja el esfuerzo del sistema judicial peruano por responder con celeridad y firmeza ante nuevas formas de criminalidad patrimonial, donde el uso de medios digitales altera los métodos tradicionales de comisión del delito. Asimismo, el caso muestra cómo estos delitos no solo afectan a personas naturales, sino también a entidades públicas, lo que agrava su impacto social y económico.

Este hecho permite establecer un puente entre el fraude informático y los delitos contra el patrimonio, en tanto ambos tutelan el mismo bien jurídico, pero requieren una adaptación del análisis penal a las particularidades técnicas de los medios utilizados. En este sentido, el caso constituye un precedente útil para comprender cómo la imputación objetiva debe aplicarse con criterio técnico-jurídico en escenarios donde los daños patrimoniales son causados mediante herramientas digitales.

En relación con el objetivo 2

Tabla 5

Caso "Condena anticipada por fraude informático"

FUENTE DOCUMENTAL	CONTENIDO DE LA FUENTE DOCUMENTAL	ANÁLISIS DEL CONTENIDO DE LA FUENTE DOCUMENTAL	CONCLUSIÓN
Fecha: 20/04/2022 Institución: Primer Despacho de la fiscalía provincial Corporativa Especializada en Ciberdelincuencia de Lima Centro Caso: Condena anticipada por el delito de fraude informático Sentenciada: Úrsula Durand Valdez Víctima: Cliente de un salón de belleza	Se describe un caso de fraude informático en el que Úrsula Durand Valdez, una trabajadora de una peluquería, fue condenada anticipadamente a dos años y seis meses de prisión suspendida por tomar fotografías de la tarjeta de crédito de una clienta y utilizar los datos para comprar un celular en una tienda virtual. La sentencia también incluye el cumplimiento de reglas de conducta, el pago de una multa de 333.5 soles y una reparación civil de 2,009 soles a favor de la víctima.	Vulnerabilidad en Transacciones Cotidianas**:** La fuente destaca cómo una simple transacción en un salón de belleza puede ser explotada para cometer un fraude, subrayando la necesidad de estar atentos al manejo de nuestras tarjetas de crédito. Evidencia y Procedimiento Legal**:** La condena se basó en pruebas concretas, incluyendo imágenes de cámaras de seguridad que mostraban a la perpetradora tomando fotografías de la tarjeta. Esto resalta la importancia de las evidencias visuales y digitales en la resolución de casos de ciberdelincuencia. Impacto y Responsabilidad**:** La condena no solo incluye una sentencia de prisión suspendida, sino también multas y reparaciones civiles, enfatizando la gravedad del delito y la responsabilidad financiera del delincuente hacia la víctima. Medidas Preventivas**:** El caso subraya la necesidad de implementar medidas preventivas tanto por parte de los consumidores como de los establecimientos comerciales, como el uso de sistemas de pago más seguros y la vigilancia constante del uso de tarjetas de crédito.	La condena anticipada de Úrsula Durand Valdez por fraude informático resalta la importancia de la seguridad en el manejo de datos personales y financieros. La resolución del caso muestra cómo la evidencia digital y visual puede ser crucial para la justicia en delitos cibernéticos. Este incidente subraya la necesidad de mayores medidas preventivas y educativas para proteger a los consumidores y sancionar adecuadamente a los infractores.

Nota. Elaboración propia.

Interpretación:

El caso de Úrsula Durand Valdez, condenada por tomar fotografías de la tarjeta de crédito de una clienta y utilizar esos datos para realizar compras en línea, evidencia las dificultades que enfrenta el sistema penal al intentar encuadrar estas nuevas formas de apropiación patrimonial dentro del marco del delito tradicional de hurto. En términos clásicos, el hurto requiere el apoderamiento ilegítimo de un bien mueble sin violencia, con la característica de que el agente debe tomar físicamente la cosa mueble ajena. Sin embargo, en este caso, la agente no sustrae físicamente ningún objeto, sino que copia datos digitales que luego utiliza para obtener un beneficio económico. Esta modalidad de apoderamiento, desmaterializada y mediada por tecnología, presenta una ruptura con la configuración típica del hurto, dificultando su aplicación literal en el procedimiento penal.

Aquí es donde la imputación objetiva cobra un rol esencial. Desde esta perspectiva, el comportamiento de la autora crea un riesgo jurídicamente desaprobado (capturar y usar datos personales sin autorización) que se materializa en un resultado lesivo previsible y evitable (el perjuicio económico de la víctima). Aunque no existe apoderamiento físico, el bien jurídico protegido el patrimonio resulta claramente afectado. Por tanto, el análisis debe centrarse en la lesividad efectiva y el control del hecho, más que en la modalidad física de la apropiación.

Esta interpretación permite reconocer que el fraude informático puede simular en muchos aspectos al hurto, pero al no ajustarse plenamente a su estructura legal, se vuelve necesaria una reconfiguración del análisis penal a través de doctrinas como la imputación objetiva. Además, refuerza la importancia de adaptar el sistema procesal a nuevas formas de criminalidad patrimonial, que utilizan medios digitales para sortear las limitaciones de los tipos penales tradicionales. En síntesis, el caso de Durand Valdez demuestra que el fraude informático desafía la tipicidad del hurto al sustituir la sustracción física por apropiación de datos. La imputación objetiva permite resolver este vacío al centrar el juicio de responsabilidad en el riesgo creado, el dominio del hecho y el resultado lesivo, lo que permite imputar de forma adecuada conductas que de otro modo quedarían impunes bajo un análisis típico estricto.

En relación con el objetivo 3:

Tabla 6

Caso "Uso de criptomonedas en delito de fraude informático"

FUENTE DOCUMENTAL	CONTENIDO DE LA FUENTE DOCUMENTAL	ANÁLISIS DEL CONTENIDO DE LA FUENTE DOCUMENTAL	CONCLUSIÓN
Caso: Primer sentencia por fraude informático con criptomonedas en Perú. Sentenciado: José Leonell Llanos Rodríguez. Condena: Tres años y cuatro meses de prisión. Acción Delictiva: Desvío de 6,500 soles a una billetera electrónica de criptomonedas mediante datos bancarios obtenidos ilícitamente. Investigación: Fiscalía Especializada en Ciberdelincuencia de Lima Centro, liderada por la fiscal Angélica Pérez Asencio. Método: Uso de un exchange para convertir datos bancarios en criptomonedas, evitando el rastreo mediante una billetera electrónica.	La fuente documental informa sobre la primera sentencia en Perú por delito de fraude informático mediante el uso de criptomonedas. José Leonell Llanos Rodríguez fue condenado a tres años y cuatro meses de prisión por desviar 6,500 soles hacia una billetera electrónica de criptomonedas, utilizando datos bancarios obtenidos de manera ilegal. La investigación estuvo a cargo de la Fiscalía Especializada en Ciberdelincuencia de Lima Centro, dirigida por la fiscal Angélica Pérez Asencio. El caso resalta el uso de un exchange digital para convertir datos bancarios en criptomonedas y la utilización de una billetera electrónica para recibir los fondos, evitando así ser identificado fácilmente.	El caso revela varias dimensiones importantes del fraude informático en la era de las criptomonedas. Primero, muestra cómo los delincuentes pueden aprovechar las plataformas digitales para realizar transferencias fraudulentas de manera relativamente anónima. El uso de tecnologías como los exchanges y las billeteras electrónicas plantea desafíos adicionales para la identificación y persecución de los culpables, evidenciando la necesidad de herramientas avanzadas de investigación y seguimiento digital por parte de las autoridades competentes. Además, la condena de José Leonell Llanos Rodríguez destaca la seriedad con la que el sistema judicial peruano aborda los delitos cibernéticos, subrayando la importancia de las sanciones penales como medida disuasoria y correctiva. Este caso también resalta la labor especializada de la Fiscalía en Ciberdelincuencia de Lima Centro, que emplea técnicas avanzadas para investigar y documentar casos complejos de fraude digital.	La sentencia de José Leonell Llanos Rodríguez por fraude informático con criptomonedas establece un precedente significativo en la persecución de delitos financieros en el entorno digital. Además de la condena penal, esta resolución destaca la importancia de la especialización y la capacitación dentro del sistema judicial para enfrentar efectivamente los crímenes cibernéticos. Es crucial continuar fortaleciendo las capacidades investigativas y legislativas para adaptarse a la evolución constante de las tecnologías y proteger así la seguridad financiera y digital de los ciudadanos.

Nota. Elaboración propia.

Interpretación:

El caso de José Leonell Llanos Rodríguez, condenado por desviar 6,500 soles mediante el uso de criptomonedas, representa un claro ejemplo de cómo las conductas propias del fraude informático desafían la estructura clásica del delito de estafa, especialmente en lo que respecta a la aplicación de la imputación objetiva. Tradicionalmente, la estafa exige la presencia de un engaño directo y personal, dirigido a inducir en error a la víctima para que esta realice un acto de disposición patrimonial. Sin embargo, en el presente caso, el apoderamiento se produce a través de medios tecnológicos acceso indebido a datos bancarios, uso de exchanges digitales y billeteras electrónicas, sin una interacción física o directa entre el autor y la víctima. Este desplazamiento del engaño hacia una dimensión técnica y automatizada genera una dificultad importante en los procedimientos penales, pues complica la identificación del dolo específico y la relación causal entre la conducta y el perjuicio.

Aquí es donde cobra relevancia la imputación objetiva como herramienta jurídica para atribuir responsabilidad penal de forma racional. La creación de un riesgo no permitido, materializado en la sustracción de fondos mediante el uso de tecnología, permite superar las limitaciones del tipo penal de estafa, focalizando el análisis en la peligrosidad del comportamiento y su resultado, en lugar de en los elementos subjetivos tradicionales. Asimismo, este caso visibiliza cómo el anonimato y la descentralización propios de las criptomonedas dificultan el rastreo de operaciones fraudulentas, lo que a su vez evidencia la necesidad de un sistema penal especializado, con técnicas y criterios modernos de imputación y prueba. La actuación de la Fiscalía Especializada en Ciberdelincuencia fue determinante para reconstruir la cadena de eventos delictivos y lograr una condena eficaz, lo que resalta la importancia de la especialización del sistema judicial en estos contextos.

En conclusión, este caso permite observar que los delitos informáticos, pese a compartir características funcionales con la estafa tradicional, requieren de una redefinición de sus elementos jurídicos sustanciales. La imputación objetiva ofrece una vía coherente y flexible para atribuir responsabilidad penal en escenarios donde el engaño, aunque no sea personal, resulta igualmente perjudicial y doloso.

3.2. Resultados de Análisis de jurisprudencias

En relación con el Objetivo General

Tabla 7

Pleno. sentencia 1100/2020 del tribunal constitucional.

FUENTE JURISPRUDENCIAL	CONTENIDO DE LA FUENTE JURISPRUDENCIAL	ANÁLISIS DEL CONTENIDO DE LA FUENTE JURISPRUDENCIAL	CONCLUSIÓN
Sentencia del Tribunal Constitucional del Perú, específicamente la Sentencia del Pleno del Tribunal Constitucional del 10 de diciembre de 2020, en el Expediente 01189-2019-PHC/TC.	En la sesión del Pleno del Tribunal Constitucional del 10 de diciembre de 2020, se emitió la sentencia que declaró INFUNDADA la demanda de hábeas corpus presentada por don William Benardino García Rosales a favor de Marcos Morales Vargas. La demanda cuestionaba la legalidad de una condena por fraude informático y falsificación de firma en documento privado, argumentando la aplicación retroactiva de la Ley 30096.	La sentencia analiza la aplicación del principio de legalidad penal, destacando que la Ley 30096, que sanciona el fraude informático, estaba vigente al momento de los hechos delictivos. Se discute la interpretación de los elementos constitutivos del delito y la adecuación de la norma aplicada por los tribunales ordinarios.	El Tribunal Constitucional concluyó que no hubo vulneración del principio de legalidad penal en el proceso seguido contra Marcos Morales Vargas. La sentencia destaca la importancia de la aplicación correcta de la normativa vigente al momento de los hechos para garantizar el debido proceso y la tutela judicial efectiva.

Nota. Elaboración propia.

Interpretación:

La Sentencia del Tribunal Constitucional en el Expediente 01189-2019-PHC/TC del 10 de diciembre de 2020 aborda la demanda de hábeas corpus presentada por William Benardino García Rosales a favor de Marcos Morales Vargas, quien impugnó la legalidad de su condena por fraude informático y falsificación de firma en documento privado. El fallo sostiene que la Ley 30096, que penaliza el fraude informático, estaba en vigor al momento de los hechos delictivos, validando así la aplicación retroactiva de esta ley por los tribunales ordinarios. La sentencia destaca la importancia de la interpretación correcta de los elementos constitutivos del delito y la adecuación de la normativa vigente para asegurar el debido proceso y la tutela judicial efectiva, concluyendo que no se vulneró el principio de legalidad penal en el proceso contra Marcos Morales Vargas.

Este caso permite comprender cómo el Tribunal Constitucional legitima la aplicación del tipo penal de fraude informático, dejando en claro que la norma (Ley 30096) se encontraba vigente al momento de los hechos. Aunque no se analiza directamente la imputación objetiva, esta decisión refuerza el marco normativo desde el cual se puede construir dicha imputación. La correcta identificación del momento delictivo es fundamental para determinar si el riesgo penalmente desaprobado es atribuible al sujeto activo.

En relación con el objetivo general

Tabla 8

Recurso de casación n.º 3330-2022/ el santa.

FUENTE JURISPRUDENCIAL	CONTENIDO DE LA FUENTE JURISPRUDENCIAL	ANÁLISIS DEL CONTENIDO DE LA FUENTE JURISPRUDENCIAL	CONCLUSIÓN
Sentencia de Casación, Lima 14 de febrero de 2024, recurso de casación *N.º 3330-2022/ El Santa.*	Marco André Gómez García presentó un recurso de casación alegando la vulneración de normas procesales y sustantivas, impugnando la sentencia del 20 de octubre de 2022 que confirmó su condena previa del 26 de mayo del mismo año. Fue hallado culpable de uso de documento falso y fraude informático, recibiendo una pena de nueve años y seis meses de prisión, una multa de 130 días y el pago de una reparación civil de S/ 180,000 al Banco BBVA, además de S/ 500 a cada uno de los doce agraviados mencionados.	Partes Involucradas: El recurso de casación involucra a un imputado acusado de fraude informático y falsedad ideológica. Cuestión Legal: Determinar si se configuró el delito de fraude informático y falsedad ideológica basado en el uso de documentos falsos para manipular el sistema informático de un banco. Interpretación de Normas: El tribunal evalúa la aplicación de los tipos penales de fraude informático y falsedad ideológica en relación con el uso de documentos falsos para manipular un sistema informático bancario. Argumentos Legales: Se establece que la manipulación del sistema informático mediante documentos falsos constituye una unidad de acción delictiva. Decisión Judicial: Se concluye que el imputado utilizó documentos falsos para alterar el sistema informático del banco, causando un perjuicio patrimonial.	El recurso de casación presentado por Marco André Gómez García se centra en dos principales causales: el quebrantamiento de precepto procesal y la infracción de precepto material. En primer lugar, se argumenta que durante el proceso judicial pudo haber ocurrido errores en la aplicación de normas procedimentales. Estos errores podrían incluir desde la admisión indebida de pruebas hasta posibles irregularidades que podrían haber afectado los derechos de defensa del acusado. Por otro lado, se alega una posible interpretación incorrecta o inadecuada de normas sustantivas aplicables al caso. Esto sugiere que las leyes pertinentes podrían no haber sido correctamente aplicadas o interpretadas en relación con las acciones atribuidas a Marco André Gómez García.

Nota. Elaboración propia.

Interpretación:

El recurso de casación interpuesto por Marco André Gómez García se centra en dos aspectos principales: el quebrantamiento de precepto procesal y la infracción de precepto material. Estas son las bases legales sobre las cuales se argumenta que hubo errores en el proceso judicial que podrían haber afectado la validez de la sentencia impuesta. El quebrantamiento de precepto procesal se refiere a posibles errores en la aplicación de las normas procedimentales durante el juicio, mientras que la infracción de precepto material sugiere que pudo haber habido una interpretación incorrecta o inadecuada de las normas sustantivas o de fondo aplicables al caso.

La conducta del imputado, manipulación informática mediante el uso de documentos falsos permite aplicar directamente los criterios de la imputación objetiva: creación de un riesgo no permitido y materialización del daño patrimonial. El tribunal considera que dicha conducta tiene un nexo de causalidad y dominio funcional sobre el resultado, elementos centrales en la doctrina de la imputación objetiva, lo que justifica plenamente la sanción penal por fraude informático.

En relación con el objetivo 3

Tabla 9

Recurso de casación n° 2872-2022/san martín.

FUENTE JURISPRUDENCIAL	CONTENIDO DE LA FUENTE JURISPRUDENCIAL	ANÁLISIS DEL CONTENIDO DE LA FUENTE JURISPRUDENCIAL	CONCLUSIÓN
Sentencia de casación, recurso por quebrantamiento por precepto procesal, casación N° 2872-2022/San Martín.	La Sentencia Casatoria N°2872-2022/San Martín establece principios fundamentales relacionados con el principio de continuidad del juicio, la proporcionalidad en la aplicación de nulidades procesales, y la interpretación de los tipos delictivos de fraude informático y falsedad material impropia. Analiza cómo el tiempo de interrupción del juicio puede afectar la memoria de los actos y las garantías procesales fundamentales como la inmediación y la veracidad del esclarecimiento del delito. Expone criterios doctrinales sobre la subsanación de nulidades relativas en el proceso penal, particularmente en relación con la continuidad del debate judicial y la actuación de pruebas.	La jurisprudencia citada proporciona directrices claras sobre cómo deben interpretarse y aplicarse los principios procesales mencionados en casos similares al presente. Destaca la importancia de evaluar el impacto del tiempo de interrupción en la integridad del proceso judicial y la equidad procesal. Define el marco jurídico para entender las unidades de acción en delitos complejos como el fraude informático y la falsedad ideológica, haciendo énfasis en la manipulación de sistemas informáticos mediante el uso de documentos falsos.	En virtud de la Sentencia Casatoria N°2872-2022/San Martín, se concluye que el presente caso debe evaluarse considerando los principios de continuidad del juicio, proporcionalidad en la aplicación de nulidades procesales y la interpretación precisa de los tipos delictivos involucrados. Se establece que el imputado, al utilizar documentos falsos para manipular el sistema informático del Banco agraviado, actuó en unidad de acción conforme a los tipos delictivos de fraude informático y falsedad material impropia. La subsanación de las nulidades relativas debe considerarse según los lineamientos doctrinarios y jurisprudenciales expuestos, garantizando así la regularidad y validez del proceso judicial.

Nota. Elaboración propia.

Interpretación:

La interpretación del caso se fundamenta en la jurisprudencia citada, que destaca la importancia del principio de continuidad del juicio para evitar distorsiones en la memoria procesal debido a interrupciones prolongadas. Además, se enfatiza la necesidad de aplicar el principio de proporcionalidad al evaluar las nulidades procesales, considerando el impacto en garantías fundamentales como la inmediación y la veracidad del esclarecimiento del delito. En cuanto a la naturaleza de los delitos imputados, se concluye que las acciones del acusado constituyen una unidad de acción, dado que el uso de documentos falsos para manipular sistemas informáticos y obtener beneficios ilícitos está cohesionado por una única intención criminal.

El caso muestra cómo el uso de documentos falsos para manipular un sistema informático crea una figura similar a la estafa, pero sin el engaño directo a una persona natural, como en los tipos clásicos. Esto evidencia una de las principales dificultades en la imputación objetiva: la identificación de un riesgo típicamente desaprobado en delitos patrimoniales con estructura automatizada. El tribunal aborda la unidad de acción en delitos complejos, lo que apoya la necesidad de adaptar la imputación a nuevas formas delictivas digitales.

3.3 Resultado del análisis de entrevistas

Así también, examinaremos las respuestas de la entrevista realizada a nuestros expertos, con el propósito de respaldar el objetivo de la investigación, con el fin de ofrecer una explicación clara y fundamentada sobre la aplicación de la Imputación Objetiva en el delito de fraude informático frente a los delitos contra el patrimonio en Lima, 2024.

Con relación al objetivo general

1. ¿Cuáles son los estándares de imputación objetiva que deben establecerse en la determinación del delito de fraude informático?

El Dr. Quispe (2024), comenta que en las proposiciones fácticas en cuanto a la imputación objetiva es relevante la precisión y desarrollo del medio comisivo (diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático). En el caso de una pluralidad de imputados las conducta o rol que habría desarrollado cada uno la ejecución del delito, conforme con la Casación 247-2018.

A su vez, la Dra. Gálvez (2024), señala que los estándares son entendidos como modelo o referencia, respecto a la imputación objetiva que verifica el comportamiento, es decir si la conducta es Típica, la imputación objetiva es el resultado es decir lesivo, sea producto del comportamiento imputado, y sobre la imputación subjetiva como estándares sería verificar el dolo, la culpa o el error.

Así también, la Dra. Robles (2024), añade que en el caso de la imputación objetiva se valora los elementos del delito tales como la acción típica, el verbo rector, el sujeto activo, el sujeto pasivo, el grado de participación y por el lado del tipo subjetivo el dolo, esto es como conocimiento, de que el agente está realizando el tipo de forma consciente, sin ninguna causa de justificación.

La Abogada Durand (2024), menciona que la imputación objetiva es aquella figura del derecho penal, el cual se aplica para sancionar la punibilidad de una conducta cuyos efectos alteran el entorno o las personas sobre los cuales recae, es decir las conductas que generan consecuencias que pueden ser catalogadas como punibles, en el caso concreto cuando el agente sistemáticamente realiza con intención dolosa o delictiva el obtener de forma ilegítima un beneficio económico para uno mismo o para otro; mientras que la imputación subjetiva consiste en valorar si el agente conoce el riesgo de su conducta, es decir si el agente actúa con dolo o no; en ese orden de ideas se dice que la imputación subjetiva es aquella atribución que se da a la conducta del sujeto de los elementos subjetivos del delito, dicho en otras palabras la conciencia de realizar los actos del tipo, en el caso en concreto, si el agente era o no consiente que al realizar manipulaciones de delitos informáticos estas conductas acarrearía.

Asimismo, la abogada Fernández (2024), refiere que la conducta típica del delito de fraude informático, en sentido estricto, afecta en sistema de tratamientos automatizados de información (a través de las tecnologías de la información o de la comunicación) y tiene como fundamentos típicos en perjuicio de terceros (para sí o para otro). En ese sentido puede confundirse o tener similitudes con otros delitos informáticos, cuando se enfoca de una perspectiva amplia, no obstante, ello, la diferencia principal es por el uso del medio comisivo del delito de fraude informático, desde una interpretación escrita para la diferenciación con los demás delitos informáticos contra el patrimonio.

Convergencias:

- Todos los entrevistados coinciden en que la imputación objetiva requiere evaluar la conducta típica delictiva, los medios comisivos, y que debe existir una relación de causalidad entre la conducta y el resultado lesivo.
- De los 5 entrevistados 4 enfatizan el papel del dolo como elemento del tipo subjetivo, es decir, que el agente debe tener conocimiento y voluntad de su actuar delictivo (Gálvez, Robles, Durand, Fernández). Por último 3 de los entrevistados destacan que el fraude informático implica acciones específicas como alteración, borrado o manipulación de datos informáticos, que deben ser individualizadas en la imputación objetiva (Quispe, Robles, Fernández).

Divergencias:

- El entrevistado el Dr. Quispe hace énfasis en la pluralidad de imputados y el análisis de roles conforme a la jurisprudencia (Casación 247-2018), las Dras. Durand y Fernández enfatizan más bien el análisis del resultado y su afectación al entorno o a terceros.
- Hay diferencias en el enfoque, algunos se centran más en lo doctrinal/técnico (Robles, Gálvez), mientras que otros lo vinculan a la práctica jurídica y casuística concreta (Quispe, Durand).

2. ¿Cuáles cree que son los desafíos que se enfrentan al procesar casos de fraude informático en comparación con otros delitos patrimoniales?

El Dr. Quispe menciona que en estos casos dada las singularidades del tipo penal, no es suficiente con los actos de investigación tradicionales para el esclarecimiento del hecho (declaraciones, documentos) sino que debe optarse por diligencias especiales (levantamiento del secreto bancario y de comunicaciones, realización de pericias, geolocalización, entre otros). La pericia informática es clave, lo que exige a los operadores jurídicos poseer un cierto conocimiento del manejo de las herramientas informáticas para comprender el caso.

La Dra. Gálvez señala que los desafíos serían la identificación de los sujetos activos debido al uso de medios informáticos.

Así también, la Dra. Robles señala que es necesario el conocimiento especializado de los operadores de justicia en las nuevas tecnologías de la información y de poder interpretar los resultados de las diferentes pericias tecnológicas.

La Abg. Durand, opina sobre la legislación ha ido evolucionando para abordar los desafíos del fraude informático. En 2013, se promulgó la Ley Nº 30096, conocida como la "Ley de Delitos Informáticos", que establece disposiciones específicas para penalizar diversas conductas delictivas en el ámbito digital, incluyendo el fraude informático. En general, la efectividad de la legislación peruana en la lucha contra el fraude informático depende no solo de la existencia de leyes específicas, sino también de la capacidad de las autoridades para aplicarlas de manera efectiva, así como de la cooperación internacional en casos que involucren a actores fuera del país.

La Abg. Fernández señala que el problema no es si es o no suficiente las legislación actual frente a la lucha o desafío que conlleva el combatir el fraude informático, si no que resulta ser necesario establecer técnicas de investigación hasta cooperación interinstitucional (PNP, MISNISTERIO PRUBLICO, BANCOS Y OTROS) Que faciliten tanto el hallazgo de la ruta del dinero, de los responsables directos, puesto que mientras más puestos tecnológicos existan mayor será el campo de afectación del delincuente, mientras que el estado se queda relegado e incapaz de afrontar dicha realidad.

Convergencias:

- Todos los entrevistados reconocen que el fraude informático plantea mayores desafíos técnicos en comparación con los delitos patrimoniales tradicionales.

- Existe acuerdo en que se requieren conocimientos especializados y herramientas tecnológicas para abordar este tipo penal (Quispe, Robles, Gálvez).
- Se menciona la necesidad de pericias informáticas y técnicas de investigación más complejas como elementos imprescindibles (Quispe, Fernández).

Divergencias:

- Mientras los 2 entrevistados la Dra. Robles y el Dr. Quispe destacan la necesidad de capacitación de los operadores de justicia, las abogadas Durand y Fernández se enfocan en los vacíos o limitaciones del sistema legal y la cooperación interinstitucional.
- La Jueza Gálvez, menciona que el principal desafío es la identificación de los autores materiales por el uso anónimo de medios informáticos, mientras que otros hacen hincapié en la efectividad de la legislación y la respuesta del Estado.

3. ¿Cuáles son los elementos típicos (subjetivos y objetivos) del delito de fraude informático en su discriminación con los delitos patrimoniales?

Según el Dr. Quispe (2024), refiere que el delito de fraude informático en cuanto a sus elementos objetivos exige primero que el agente procure un provecho ilícito, esto es, una ventaja o un enriquecimiento que puede para sí o para tercero. Este provecho debe ser obtenido por cualquiera de los medios que prevé el tipo penal (diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático). En ese marco, resulta trascendente identificar alguna conducta vinculada al sistema informático. La pericia informática en estos casos puede aclarar el panorama. Respecto al aspecto subjetivo el

tipo penal resalta que la conducta debe ser deliberada e ilegítima, lo cual revelaría que el dolo debe ser directo.

La Dra. Celeste (2024), detalla en este orden lo siguiente:

Elementos subjetivos → DOLO.

Elementos objetivos → Conducta sea típica, antijurídica culpa y punible.

Típica → que el delito de fraude informático esté descrito como tipo objetivo: sujeto, objeto, conducta y subjetivo: dolo o culpa.

Antijurídica→ conducta desplegada del "engaño" sea contraria a la ley.

Culpable → La reprochabilidad de la conducta de fraude informático.

Punible → dicha conducta merece una pena.

La Dra. Ramos (2024), menciona que entre los elementos objetivos típicos tenemos al sujeto activo, el provecho ilícito, el verbo rector “procura”, los medios de realización tales como: alteración, borrado, supresión, alteración, clonación de datos informáticos, etc., mientras que elemento subjetivo principal es el dolo, es decir el conocimiento del agente para cometer el delito.

Según Durand (2024), refiere que el delito de extorsión el sujeto pasivo hace la entrega del bien por la intimidación, amenaza o violencia que realizar el sujeto activo para conseguir una ventaja económica; y por último el delito de hurto en cuando el agente se apodera ilegítimamente de un elemento ajeno sin utilizar la violencia.

La Dra. Fernández (2024), menciona que, el delito de fraude informático se distingue de los delitos patrimoniales por sus elementos típicos, tanto objetivos como subjetivos. En términos objetivos, el fraude informático implica el uso de medios

informáticos o electrónicos para perpetrar el engaño. Esto puede manifestarse en formas como el acceso no autorizado a sistemas informáticos, la alteración de datos o la realización de transacciones fraudulentas a través de redes digitales. Estos elementos objetivos subrayan la importancia del componente tecnológico en la comisión del delito. Por otro lado, los elementos subjetivos del fraude informático incluyen la intención específica de cometer fraude mediante el uso de estos medios tecnológicos. Es fundamental demostrar que el autor actuó con conocimiento y voluntad de engañar o causar perjuicio utilizando la tecnología como herramienta principal. Esta intención subjetiva distingue el fraude informático de otros delitos patrimoniales, donde los medios tradicionales pueden ser empleados de manera distinta y con motivaciones diversas.

Convergencias:

- Todos los entrevistados reconocen que el fraude informático tiene elementos típicos particulares, tanto en el plano objetivo (conducta, medio informático, resultado) como subjetivo (dolo específico).
- Se coincide en que el elemento tecnológico es esencial para distinguir este delito de otros patrimoniales como hurto o extorsión (Fernández, Quispe, Ramos).

Divergencias:

- Mientras la Dra. Celeste y la Dra. Ramos abordan los elementos típicos desde una estructura penal clásica (típica, antijurídica, culpable y punible), la Abogada Durand hace una comparación directa con otros delitos patrimoniales (hurto, extorsión).

- Algunos enfoques son más conceptuales y doctrinarios (Celeste, Robles), y otros más casuísticos y prácticos (Durand, Fernández).

Interpretación en base al objetivo general:

Respecto a la primera pregunta sobre los estándares de imputación objetiva en el delito de fraude informático, se identificó una convergencia general en cuanto a que la conducta debe ser típica, dolosa y lesiva, y que debe evaluarse el medio comisivo utilizado, como la manipulación de sistemas informáticos. No obstante, se observó una divergencia en los enfoques, pues mientras algunos entrevistados se centraron en el análisis técnico-jurídico del tipo penal, otros priorizaron los efectos prácticos y la jurisprudencia aplicable.

En cuanto a los desafíos al procesar casos de fraude informático, todos los entrevistados coincidieron en que estos delitos requieren mayor especialización técnica, así como la utilización de herramientas de investigación avanzadas, lo que evidencia una convergencia significativa en este aspecto. Sin embargo, se presentaron diferencias de énfasis: algunos resaltaron las limitaciones del sistema legal, mientras otros destacaron la necesidad de fortalecer la cooperación institucional e internacional.

Sobre los elementos típicos del delito de fraude informático en comparación con otros delitos patrimoniales, hubo una clara convergencia al señalar que el uso de medios tecnológicos y la intención dolosa son aspectos distintivos fundamentales. Pese a ello, se identificaron divergencias en la forma de abordar la estructura típica, variando entre enfoques doctrinales y comparativos con otros delitos como el hurto o la extorsión.

Con relación al objetivo específico 1

1. ¿Cómo se diferencia legalmente el fraude informático de otras figuras delictivas relacionadas, como el robo?

Según Quispe (2024), el apoderamiento de dinero en los delitos patrimoniales en la actualidad puede cometerse a través de transferencias bancarias no autorizadas. Sin embargo, el medio comisivo a través del cual se produce este apoderamiento puede ser de variada forma: por violencia, destreza, obtención fraudulenta de claves, o de clonación o manipulación del sistema informático, entre otros. Es por ello que la diferencia delictiva en estos casos radica en el medio comisivo a través del cual se realiza el acto de apoderamiento.

Gálvez (2024), añade que el fraude informático de las otras figuras delictivas se diferencia por el uso de sistemas informáticos y que apareció a raíz de los cambios de la globalización.

Por otro lado, la Dra. Robles (2024), menciona la ley N° 30096 sobre delitos informáticos, establece en su artículo 8° fraude informático, como al sujeto que deliberadamente procura para sí o un tercero un provecho ilícito, alterando, suprimiendo, etc. Los datos informáticos, por lo que podemos advertir que la diferencia se centra en los bienes no corporales de apropiación y que se encuentran en dispositivos informáticos.

Asimismo, la Dra. Durand añade que, el delito de fraude informático se diferencia de otros delitos, porque este delito para su configuración requiere que el agente realice manipulaciones de datos de sistema informativo puede ser a través del uso de computadoras, internet u otros dispositivos y con ello defraudar recursos a personas u organizaciones; a diferencia del delito de robo que se requiere la sustracción del bien ejerciendo violencia.

La Dra. Fernández (2024), añade que, si bien el delito de fraude informático, así como los delitos de robo tiene como bien jurídico protegido al patrimonio, esto es, el delito de fraude informático supone un perjuicio patrimonial mediante la manipulación o alteración de datos o sistemas informáticos.

Convergencias:

- Todos los entrevistados coinciden en que el medio comisivo es el principal criterio diferenciador entre el fraude informático y el robo.
- Hay acuerdo en que el fraude informático se ejecuta mediante la manipulación de sistemas o datos digitales, mientras que el robo involucra violencia o amenaza física sobre bienes materiales (Durand, Quispe, Fernández).
- Se reconoce que ambos delitos afectan el mismo bien jurídico protegido (el patrimonio), aunque de formas distintas (Robles, Fernández).

Divergencias:

- Algunos entrevistados, como Gálvez, vinculan esta diferenciación al contexto de globalización y evolución tecnológica, mientras que otros, como Robles y Durand, se enfocan en los aspectos normativos y técnicos del tipo penal.
- Mientras Robles se centra en la Ley N° 30096, Quispe se enfoca en los modos de apoderamiento según el caso concreto.

2. ¿Cuáles son las principales dificultades que enfrenta la aplicación de la imputación objetiva en los procedimientos por robo en casos de fraude informático?

El Dr. Quispe (2024), menciona que la principal dificultad radica en la dificultad para identificar el daño directo en los fraudes informáticos. En el contexto del robo tradicional, el perjuicio es claro, pues involucra un bien tangible, pero en los casos de fraude informático, los bienes involucrados son intangibles, lo que complica la

determinación de la imputación objetiva. Esto plantea problemas en cuanto a la valoración del perjuicio y la forma de asociarlo a la conducta del imputado.

Según Gálvez (2024), sostiene que, uno de los principales retos es el análisis de la causalidad. En el fraude informático, las intervenciones tecnológicas a menudo son complejas, y la cadena causal entre el acto delictivo y el resultado es difícil de establecer. Esto afecta la imputación objetiva, ya que es complicado determinar si la conducta del acusado fue la causa directa del daño o si existieron otros factores tecnológicos o humanos que influyeron en el resultado.

La Dra. Robles, refiere que un obstáculo importante es la naturaleza del bien jurídico protegido. En los delitos informáticos, el bien protegido es la integridad del sistema informático y la confianza en las transacciones digitales. Esto difiere significativamente de los robos tradicionales, donde el bien material es el foco. En consecuencia, aplicar la imputación objetiva en este contexto puede resultar complicado, ya que el daño no siempre es inmediatamente visible o tangible.

Según Durand (2024), señala que la fragmentación y anonimato de las transacciones digitales son un desafío para la imputación objetiva en casos de fraude informático. Los acusados pueden actuar a través de múltiples capas de intermediarios o utilizar tecnología que oculta su identidad. Esto complica la identificación de la relación directa entre el acto delictivo y el perjuicio ocasionado, lo cual es esencial para una imputación objetiva clara.

La Abogada Fernández, enfatiza que, la dificultad en la aplicación de la imputación objetiva en fraudes informáticos también radica en la velocidad con la que los sistemas digitales permiten la circulación del dinero o bienes. La rapidez de las transacciones electrónicas puede hacer que el perjuicio sea más difuso y disperso, lo que

dificulta atribuir directamente el resultado del fraude a una acción específica de un acusado, generando incertidumbre en la imputación objetiva.

Convergencias:

- Todos los entrevistados coinciden en que la imputación objetiva es más compleja en el fraude informático que en el robo tradicional.
- Existe acuerdo en que la intangibilidad del daño, el anonimato de los autores y la dificultad para establecer la causalidad directa son obstáculos clave (Quispe, Gálvez, Robles, Durand, Fernández).
- Se identifica como común la problemática en la atribución del resultado delictivo a una conducta individual y consciente del agente, por la complejidad técnica del medio utilizado.

Divergencias:

- Los entrevistados Quispe y Robles ponen el acento en la naturaleza del bien jurídico protegido, mientras que Durand y Fernández destacan la dimensión tecnológica: el anonimato, la fragmentación de las transacciones y la rapidez del sistema digital como barreras clave.
- La Dra. Gálvez se enfoca más en la ruptura de la cadena de causalidad directa, como problema central para la imputación objetiva.

Interpretación en base al objetivo específico 1:

Respecto a la primera pregunta, los entrevistados mostraron una posición convergente al señalar que la principal diferencia entre el delito de fraude informático y el de robo radica en el medio comisivo. Mientras el robo requiere la sustracción violenta o intimidatoria de un bien corporal, el fraude informático se ejecuta mediante la manipulación o alteración de datos digitales, sin contacto físico, pero con la intención de

obtener un provecho ilícito. Asimismo, todos señalaron que, aunque ambos delitos afectan al patrimonio como bien jurídico protegido, su estructura y ejecución son distintas, debido a los cambios tecnológicos y la creciente dependencia de sistemas digitales.

En cuanto a las dificultades que enfrenta la aplicación de la imputación objetiva en casos de fraude informático, se evidenció una coincidencia general en que estas son significativamente mayores que en el robo tradicional. Todos los expertos coincidieron en que la intangibilidad del daño, la complejidad del entorno digital, el anonimato del autor y la rapidez de las transacciones electrónicas complican el proceso de establecer una relación causal clara entre la conducta del imputado y el resultado lesivo. No obstante, se observaron matices divergentes: algunos destacaron la dificultad para identificar el daño patrimonial directo (Quispe, Robles), mientras que otros resaltaron la ruptura en la cadena de causalidad y el uso de medios tecnológicos como obstáculos determinantes (Gálvez, Durand, Fernández).

Con relación al objetivo específico 2

1. ¿Cómo se diferencia legalmente el fraude informático de otras figuras delictivas relacionadas, como el hurto?

El Dr. Quispe (2024), explica que el fraude informático se diferencia del hurto en su naturaleza y forma de ejecución. Mientras que el hurto consiste en la sustracción de bienes ajenos sin el uso de violencia, el fraude informático implica la obtención ilícita de un beneficio económico mediante el uso de tecnologías de la información y la manipulación de sistemas electrónicos o datos, sin la necesidad de apoderarse físicamente del objeto. El fraude informático se basa en la alteración o engaño de los sistemas

informáticos, mientras que el hurto es una acción física que no requiere ningún engaño, sino simplemente la apropiación indebida de bienes muebles.

Según Gálvez (2024), subraya que el fraude informático se diferencia del hurto principalmente en los métodos empleados para cometer los delitos. El fraude informático no se basa en la sustracción física de un bien, sino en el engaño o manipulación de datos o sistemas para lograr un beneficio económico, por lo general, en forma de dinero o información confidencial. A diferencia del hurto, que implica la apropiación ilícita de bienes tangibles, el fraude informático es un delito que opera sobre bienes intangibles (información, datos, acceso a sistemas, etc.), y es llevado a cabo de manera virtual. Este enfoque resalta la importancia de la tecnología y la intencionalidad fraudulenta como elementos distintivos.

La Dra. Robles (2024), explica que, aunque tanto el fraude informático como el hurto son delitos patrimoniales, se diferencian en el modo de apropiación y en el elemento engañoso del fraude. Mientras que el hurto es una conducta directa de sustracción de objetos sin el conocimiento o consentimiento de la víctima, el fraude informático se caracteriza por el uso de medios electrónicos para inducir un error en la víctima, consiguiendo que esta realice una acción en beneficio del delincuente, como la transferencia de dinero o la divulgación de información personal. La diferencia clave radica en que el fraude requiere la manipulación de información o datos y un engaño, mientras que el hurto se basa en la mera apropiación de un objeto sin que intervenga el engaño.

Según Durand (2024), plantea que la diferencia entre el fraude informático y el hurto puede entenderse a través de la causa objetiva del delito. En el fraude informático, la acción delictiva se centra en la alteración de la realidad virtual mediante el uso de

sistemas tecnológicos, como el acceso no autorizado a cuentas bancarias, sistemas informáticos o bases de datos. En cambio, el hurto se concreta en la sustracción física de un objeto sin que haya necesariamente una manipulación de sistemas o datos. Desde esta perspectiva, el fraude informático conlleva una relación más compleja con la tecnología, mientras que el hurto se basa en un comportamiento directo y material.

La Abogada Fernández (2024), en su estudio sobre la criminalidad transnacional y los delitos tecnológicos, distingue el fraude informático del hurto en función de la globalización digital. Mientras que el hurto se circunscribe a un acto de sustracción física, el fraude informático ocurre en el ámbito virtual y, por tanto, puede involucrar acciones que cruzan fronteras, dado que los sistemas informáticos son globales. La diferencia radica en que el fraude requiere de un acto de engaño digital como el acceso ilícito a redes o la suplantación de identidad, mientras que el hurto se limita a un acto físico de apropiación sin necesidad de alterar ningún sistema o utilizar medios tecnológicos.

Convergencias:

- Todos los entrevistados coinciden en que la diferencia clave radica en el medio comisivo y la naturaleza del bien afectado.
- Hay acuerdo en que el fraude informático involucra un componente tecnológico e intangible, mientras que el hurto se limita a una apropiación física (Quispe, Gálvez, Robles, Durand, Fernández).

Divergencias:

- Fernández introduce un enfoque internacional, señalando que el fraude informático puede ser transnacional y requiere un marco legal más amplio, mientras que el hurto tiene un impacto local.

- La Dra. Robles pone especial énfasis en el engaño como parte del fraude, mientras que la Dra. Durand enfoca la diferencia desde la complejidad del sistema tecnológico.

2. ¿Cuál es su opinión sobre la legislación peruana actual frente a los delitos de fraude informático en discriminación con el delito de hurto?

El Dr. Quispe (2024), refiere que es necesario reformas adicionales para operativizar el tratamiento del delito de fraude informático. Es necesario una reglamentación que defina los medios comisivos y permita su diferenciación. Asimismo, protocolos de un trabajo artículo y directivas de diligencias típicas o consustanciales del delito. Dada la naturaleza delictiva y conocimiento especiales y que se ha convertido en uno de los delitos que con mayor frecuencia se presenta debe evaluarse si se requiere una jurisdicción especializada con la creación de juzgados especializados en ciberdelincuencia.

Según Gálvez (2024), considera que es suficiente la legislación actual pero la misma irá cambiando de acuerdo con los cambios o evolución de las conductas ilícitas debido a los cambios del sistema informático, por ello dependerá del tiempo y de las meras formas de fraude informático que vayan apareciendo, sobre todo en la sociedad cambiante y que evoluciona todos los días.

La Dra. Robles, señala que si se necesitan reformas a efectos de capacitar a los operadores de justicia (jueces, fiscales, abogados, estudiantes) en esta clase de delitos, así como exponer de una forma clara cuáles son los verbos rectores para la comisión de este, evitando confusiones y lagunas jurídicas en muchos casos.

Según Durand (2024), refiere que es crucial mantenerse al día con los avances tecnológicos y las nuevas formas de fraude informático. Esto incluye definir claramente

los diferentes tipos de delitos informáticos y las acciones que los constituyen, proporcionando así una base sólida para la investigación y el enjuiciamiento. Además, se deben asignar recursos adecuados para capacitar a los funcionarios encargados de hacer cumplir la ley en la investigación de delitos informáticos y en el uso de herramientas tecnológicas especializadas para recopilar pruebas digitales. De esa forma se logrará una correcta diferenciación con delitos patrimoniales como el hurto.

La Abogada Fernández (2024), menciona que la falta de sanción a los autores de estos delitos, no se debe por la falta de aplicación o legislación particular del caso, si no que como se sabe, normalmente en los delitos informáticos los que se llegan a procesar y condenar son muchas veces los receptores y no así los autores. Ello debido a la falta de herramientas de investigación tanto para la policía como para el ministerio público que les permite ir a la par del ciber delincuente, como sí sucede en otros países.

Convergencias:

- Existe un consenso general sobre que la legislación actual requiere actualizaciones o mejoras para abordar adecuadamente el fraude informático, diferenciándolo del hurto.
- Todos señalan la necesidad de especialización, ya sea mediante capacitación (Robles, Durand), creación de juzgados especializados (Quispe) o herramientas tecnológicas para investigación (Fernández).
- Reconocen que el fraude informático exige un enfoque normativo diferente, dada su complejidad técnica y evolución constante.

Divergencias:

- La Dra. Gálvez considera que la legislación es suficiente por ahora, y que su adaptación dependerá del desarrollo de nuevas formas de fraude, lo cual contrasta con la visión más reformista e inmediata de Quispe, Robles y Durand.
- La Dra. Fernández señala que el problema no radica solo en la norma, sino en la incapacidad operativa del Estado para investigar y sancionar eficazmente a los autores principales, lo cual introduce una crítica institucional más profunda.

Interpretación en base al objetivo específico 2:

En relación con la primera pregunta, los entrevistados coincidieron en que la principal diferencia legal entre el delito de fraude informático y el hurto reside en la naturaleza de la conducta delictiva y el medio comisivo empleado. El hurto implica una sustracción directa, física y sin violencia, de un bien tangible, mientras que el fraude informático se caracteriza por el uso de medios tecnológicos para manipular datos o sistemas y obtener un provecho económico de manera ilegítima. Esta diferencia esencial se refleja también en la intangibilidad del bien afectado en el fraude informático, que suele ser dinero electrónico, datos o acceso a cuentas, lo cual exige un tratamiento jurídico especializado.

Respecto a la segunda pregunta, se evidenció una convergencia general en la necesidad de reformas legales, capacitación de operadores jurídicos y mejora de herramientas tecnológicas para enfrentar eficazmente el fraude informático. Si bien algunos como Gálvez consideran que la legislación actual es suficiente y debe ir adaptándose gradualmente a la evolución digital, la mayoría opina que se requiere una intervención más inmediata y estructurada, como la creación de juzgados especializados (Quispe), la capacitación técnica continua (Robles, Durand) y mayor inversión en

investigación digital (Fernández). Estas dificultades reflejan que, a pesar de compartir el mismo bien jurídico protegido (el patrimonio), el fraude informático plantea retos muy distintos al hurto en términos de imputación objetiva, particularmente en la identificación del autor, la prueba del dolo y la relación causal con el perjuicio económico.

Con relación al objetivo específico 3

1. ¿Cómo debería construirse la imputación en casos de pluralidad de agentes en el delito de fraude informático vinculada en delitos de estafa?

Según el Dr. Quispe (2024), menciona que, en atención al principio de imputación necesaria, debe señalarse el rol o conducta específica que habría desarrollado cada uno de los agentes, de ser posible, lo cual deberá evaluarse en cada caso en concreto. Es necesario que se señala la vinculación delictiva entre los agentes. En ese sentido, también debe establecerse si nos encontramos ante un delito cometido ocasionalmente por una pluralidad de agentes o en el marco de una banda u organización criminal. La calificación jurídica y el tratamiento punitivo varía en función a ello.

La Dra. Gálvez (2024), señala que la imputación se debe construir en mérito a cada una de Las funciones, roles y conductas desplegadas por cada uno de los sujetos activos que pertenecen a una organización criminal que obviamente tiene características para diferenciarlo de las bandas criminales.

Así también, la Dra. Ramos (2024), refiere que debería construirse como en los demás casos tradicionales de delincuencia común dado que los casos de organización criminal tienen sus propios presupuestos, y complejidad.

Asimismo, Durand (2024), añade que, en la determinación del delito de fraude informático respecto a la estafa, es crucial establecer estándares de imputación tanto objetivos como subjetivos. Desde una perspectiva objetiva, se deben considerar

elementos como el uso de medios informáticos específicos para perpetrar el fraude, como el acceso no autorizado a sistemas o la manipulación de datos electrónicos. Estos criterios objetivos son fundamentales para diferenciar el fraude informático de otros tipos de estafas que pueden ocurrir sin el uso de tecnología avanzada. Desde un punto de vista subjetivo, es esencial demostrar la intención consciente de engañar o causar perjuicio utilizando medios informáticos. Esto implica mostrar que el autor tenía conocimiento y voluntad de cometer el fraude utilizando tecnología, lo cual distingue el fraude informático de otros tipos de estafa donde la intención y el método pueden ser diferentes. Establecer estándares claros tanto objetivos como subjetivos ayuda a garantizar una aplicación coherente y efectiva de la ley en casos de fraude informático, asegurando que se aborden adecuadamente las complejidades de este tipo de delito en el ámbito digital.

Según Fernández (2024), señala que, para discriminar el delito de fraude informático de la estafa, se deben establecer estándares específicos de imputación objetiva y subjetiva. Desde un punto de vista objetivo, se debe considerar el uso de tecnología informática como un elemento central del fraude informático, implicando el acceso no autorizado a sistemas, la falsificación de datos electrónicos o la interceptación de comunicaciones digitales. Estos criterios objetivos son fundamentales para diferenciar el fraude informático de otras formas de estafa que pueden ocurrir sin el empleo de medios tecnológicos. En cuanto a la imputación subjetiva, es crucial demostrar la intención deliberada de cometer fraude utilizando medios informáticos. Esto implica evidenciar que el autor actuó con conocimiento y voluntad de engañar o causar daño aprovechando la tecnología, distinguiendo así el fraude informático de otros tipos de estafa donde los métodos y motivaciones pueden variar. Establecer estándares precisos de imputación

objetiva y subjetiva es fundamental para garantizar una aplicación coherente de la ley y una adecuada protección contra el fraude informático en el entorno digital.

Convergencias:

- Hay consenso en que la imputación debe individualizar el rol de cada agente. Tanto Quispe como Gálvez coinciden en que se deben analizar las funciones específicas de cada participante, especialmente si se trata de organizaciones criminales o bandas.
- Durand y Fernández coinciden en que debe establecerse una imputación objetiva (conducta tecnológica específica) y una imputación subjetiva (intención dolosa de causar perjuicio usando tecnología), elementos clave para diferenciar fraude informático de estafa convencional.
- Se reconoce la necesidad de criterios claros que consideren el uso de tecnología como eje de imputación (Durand, Fernández).

Divergencias:

- La Dra. Ramos propone que la imputación se construya como en la delincuencia común, sin hacer una distinción significativa, lo que contrasta con la posición más técnica y diferenciadora del resto.
- Mientras Gálvez y Quispe diferencian claramente entre bandas criminales y organizaciones, Durand y Fernández enfocan más en los criterios de imputación penal tecnológica, sin entrar en esa distinción estructural.

2. ¿Cuáles son las principales dificultades que enfrentan los órganos jurisdiccionales al procesar casos de fraude informático en comparación con en el delito de estafa?

Según el Dr. Quispe (2024), señala que una de las principales dificultades al procesar casos de fraude informático frente a casos de estafa radica en la complejidad

técnica involucrada en el análisis del delito informático. En el fraude informático, los órganos jurisdiccionales deben tener en cuenta la tecnología utilizada en el crimen, como la manipulación de sistemas, bases de datos o redes. Esto requiere conocimientos especializados en informática forense y la intervención de peritos en tecnología. A diferencia de la estafa, donde el engaño y la simulación de situaciones fraudulentas pueden ser fácilmente comprendidos por los jueces, el fraude informático exige una comprensión profunda de los sistemas electrónicos y las acciones virtuales que no son tangibles ni fácilmente verificables.

La Dra. Celeste (2024), resalta que los órganos jurisdiccionales enfrentan un desafío significativo al procesar el fraude informático, ya que la prueba digital es mucho más difusa y técnica que en los casos de estafa, donde generalmente el engaño se presenta a través de declaraciones verbales o documentales. En el fraude informático, la evidencia digital, como los registros de transacciones electrónicas, las huellas de acceso a sistemas o los códigos fuente, puede ser difícil de interpretar sin la intervención de expertos. Además, el carácter global y transnacional del fraude informático, que a menudo involucra redes internacionales y servidores distribuidos, dificulta la jurisdicción y la competencia del tribunal, lo que no ocurre con la estafa, que generalmente se comete en un ámbito local más claro.

La Dra. Ramos (2024), destaca que una de las principales dificultades radica en la determinación del engaño en el fraude informático, ya que este no siempre se manifiesta de manera explícita como en la estafa. En la estafa, el engaño se lleva a cabo a través de acciones concretas como mentir sobre la naturaleza de un producto o servicio, lo que es fácilmente identificable por los jueces. En cambio, en el fraude informático, el engaño puede consistir en una manipulación sutil de sistemas, contraseñas o la obtención de

información a través de medios como phishing o malware, lo que hace más difícil de detectar y probar. Por lo tanto, los tribunales deben analizar con detenimiento el entorno tecnológico en el que se produce el fraude, lo cual es una tarea más ardua.

Según Durand (2024), plantea que una de las principales dificultades en los casos de fraude informático es la imputación objetiva de la conducta delictiva, dado que, a diferencia de la estafa, donde el engaño tiene un contenido claro y específico, el fraude informático se basa en acciones indirectas o incluso en omisiones dentro de sistemas electrónicos. El fraude informático puede involucrar acciones que no son siempre visibles de manera tangible, como la modificación de códigos, la manipulación de transacciones electrónicas o la interceptación de datos a través de canales electrónicos. Estas acciones, aunque ilegales, son más difíciles de identificar en términos de causalidad y responsabilidad penal, lo que requiere un análisis más detallado y especializado en tecnología.

La Dra. Fernández (2024), señala que una dificultad importante en el fraude informático es el carácter descentralizado y global de los sistemas digitales. A diferencia de la estafa, que generalmente ocurre dentro de una jurisdicción específica, el fraude informático puede involucrar actores de diferentes países y sistemas informáticos dispersos a nivel mundial. Este aspecto plantea desafíos jurídicos y procesales en cuanto a la cooperación internacional, la extradición de delincuentes y el control de la evidencia digital. Además, las leyes nacionales pueden no estar completamente adaptadas a los rápidos avances tecnológicos, lo que provoca dificultades para aplicar las normativas y garantizar la protección de derechos fundamentales en un contexto global.

Convergencias:

- Todos los entrevistados coinciden en que el fraude informático presenta mayores dificultades técnicas que la estafa común: Pruebas digitales más complejas y técnicas (Celeste, Quispe, Durand).
- Necesidad de pericia tecnológica para comprender cómo se produjo el daño (Quispe, Ramos).
- Naturaleza no tangible y globalizada del delito, que exige herramientas procesales e incluso cooperación internacional (Fernández).

Divergencias:

- Las entrevistadas Celeste y Fernández profundizan en los retos jurisdiccionales y transnacionales, algo que otros entrevistados no mencionan directamente.
- Ramos y Durand ponen el foco en la dificultad para identificar el engaño, mientras Quispe y Celeste se centran más en la tecnicidad de la prueba digital.

Interpretación en base al objetivo específico 3:

Respecto a la construcción de la imputación en los casos de pluralidad de agentes dentro del delito de fraude informático vinculado con la estafa, los entrevistados coinciden en la necesidad de una individualización clara de las conductas delictivas, atendiendo a los roles funcionales y niveles de participación de cada imputado. Como destacan Quispe y Gálvez, ello es esencial para establecer si se trata de una banda o una organización criminal, lo cual modifica el tratamiento legal y punitivo.

Asimismo, se advierte una convergencia en la importancia de establecer criterios de imputación objetiva y subjetiva: la primera enfocada en los medios tecnológicos usados (alteración de sistemas, acceso ilegal, manipulación de datos), y la segunda en la

intención deliberada de causar perjuicio mediante el uso de tecnología, tal como lo afirman Durand y Fernández. No obstante, Ramos propone que se siga un esquema similar al de la delincuencia común, lo que representa un enfoque más tradicional y menos especializado.

En cuanto a las dificultades procesales, se evidencian varios retos que distinguen al fraude informático de la estafa tradicional. La estafa generalmente se basa en engaños directos y pruebas fácilmente perceptibles, mientras que el fraude informático requiere conocimientos técnicos especializados, dado que los actos delictivos pueden involucrar sistemas automatizados, códigos, transacciones virtuales y otras formas de ejecución no tangibles. Esto complica la imputación objetiva y la prueba del dolo (Quispe, Durand, Ramos). Adicionalmente, entrevistadas como Celeste y Fernández destacan la naturaleza transnacional del fraude informático, lo cual plantea problemas de jurisdicción, cooperación internacional y acceso a evidencias, un escenario que no suele presentarse en delitos de estafa tradicionales de alcance local. Así, la imputación en fraude informático exige tanto una comprensión técnica como un desarrollo normativo y procesal actualizado para enfrentar su complejidad.

CAPÍTULO IV. DISCUSIÓN Y CONCLUSIONES

En este capítulo, se procederá a realizar una interpretación comparativa de los resultados obtenidos a lo largo de la investigación con los antecedentes teóricos y estudios previos que se han expuesto en capítulos anteriores, en particular aquellos que abordan la imputación objetiva en el delito de fraude informático y su relación con los delitos contra el patrimonio. El propósito de este análisis es contrastar las conclusiones alcanzadas en la investigación de campo con las perspectivas previas sobre el marco jurídico y su aplicación, específicamente en el contexto de Lima. En este sentido, se tomarán como referencia los antecedentes de estudios previos, como los trabajos de otros expertos en el ámbito del fraude informático y la imputación objetiva, con el fin de identificar similitudes, divergencias y posibles vacíos en la aplicación de las normativas en torno a los delitos patrimoniales. Este ejercicio comparativo permitirá no solo evaluar la efectividad de los mecanismos jurídicos actuales frente al fraude informático, sino también arrojar recomendaciones fundamentadas sobre posibles mejoras y reformas para un tratamiento más adecuado de este tipo de delitos, en especial en relación con su tipificación y tratamiento en el contexto jurídico.

4.1. Interpretación Comparativa y análisis crítico

En esta sección se procedió a analizar los antecedentes, lo que ha permitido interpretar de manera integral los estudios previos.

Paguay (2020), efectuó una investigación orientada a identificar las perspectivas regulatorias concernientes a los delitos informáticos en transacciones comerciales realizadas mediante internet. La investigación constató que la Ley de Comercio Electrónico, Firmas y Mensajes de Datos que presentan insuficiencias normativas para la adecuada regulación del comercio electrónico, situación que genera un estado de

indefensión jurídica para numerosos usuarios. Esta investigación se contrapone a los resultados obtenidos en la presente investigación porque, Paguay enfatiza las limitaciones normativas en el ámbito del derecho comercial y la necesidad de actualizar el marco jurídico en materia de comercio electrónico en Ecuador, el presente estudio se enfoca en el análisis penal de la imputación objetiva aplicada al fraude informático en el Perú. En este caso, el interés no radica en la regulación del comercio electrónico, sino en cómo se configuran los elementos típicos, objetivos y subjetivos, del delito de fraude informático frente a otros delitos patrimoniales. Además, la presente investigación, desde una perspectiva casuística y jurisprudencial, demuestra que el problema no está en una ausencia normativa generalizada, sino en la aplicación e interpretación adecuada de las categorías penales tradicionales frente a nuevos medios comisivos digitales.

Chiluisa (2020), realizó un estudio para identificar las deficiencias legales en el marco jurídico ecuatoriano relacionadas con delitos informáticos que afectan a los ciudadanos. Los resultados revelan que el uso fraudulento de sistemas informáticos deja desprotegidos a personas naturales y jurídicas debido a vulnerabilidades técnicas. Esta investigación se contrapone a los resultados obtenidos en la presente investigación porque, si bien se reconoce la existencia de retos técnicos y normativos en el tratamiento del fraude informático, el presente estudio evidencia que el problema central en el contexto peruano no radica únicamente en la insuficiencia normativa, sino en la dificultad de aplicar adecuadamente la teoría de la imputación objetiva en casos concretos, especialmente al diferenciar este delito de otras figuras patrimoniales como el hurto, el robo o la estafa. Además, se observa que en el Perú existe una legislación específica como la Ley N.º 30096 que, aunque perfectible, establece un marco penal más definido, siendo el desafío

principal la interpretación judicial y el uso adecuado de herramientas tecnológicas en la investigación penal.

Cruzado (2021), evaluó el impacto del Convenio de Budapest en el sistema penal argentino, que incorporó nuevas tipificaciones delictivas. Este entorno digital diluye las fronteras nacionales debido a la naturaleza virtual de las interacciones, permitiendo que cualquier individuo opere más allá de límites geográficos tradicionales. Esta investigación se contrapone a los resultados obtenidos en la presente investigación porque, mientras Cruzado centra su estudio en la influencia de instrumentos internacionales sobre la legislación penal y la adecuación normativa de los tipos penales vinculados a delitos informáticos, el presente estudio se enfoca en el análisis de la imputación objetiva en la praxis judicial peruana. Es decir, más que analizar reformas normativas impulsadas desde tratados internacionales, esta investigación examina cómo se aplica y justifica la responsabilidad penal en casos concretos de fraude informático frente a delitos patrimoniales tradicionales, revelando una tensión entre la teoría penal y los nuevos desafíos que plantea la criminalidad digital, incluso en presencia de legislación vigente como la Ley N.º 30096.

Amaya (2024), desarrolló una investigación con el propósito de examinar las implicaciones jurídicas y los retos que enfrenta la persecución de diversos delitos cibernéticos como fraudes y estafas en el ámbito del comercio electrónico colombiano. Los hallazgos de la investigación revelan una deficiencia significativa en las capacidades institucionales del país. A pesar de las iniciativas implementadas por el gobierno colombiano para fortalecer la ciberseguridad, persiste una insuficiencia en los recursos y competencias necesarios para enfrentar eficazmente las amenazas cibernéticas. Esta investigación se contrapone a los resultados obtenidos en la presente investigación

porque, mientras Amaya resalta principalmente las limitaciones institucionales, tecnológicas y estructurales en la persecución de delitos informáticos en Colombia, el presente estudio se orienta al análisis jurídico penal de la imputación objetiva aplicada al fraude informático en el contexto peruano. Aquí, el foco no está tanto en la capacidad operativa del Estado, sino en la forma en que los operadores jurídicos interpretan, adaptan o tensan las categorías clásicas del Derecho Penal para enfrentar nuevos patrones delictivos mediados por tecnologías, en comparación con los delitos patrimoniales tradicionales. Además, se evidencia que, si bien existen limitaciones técnicas, el mayor desafío radica en los vacíos teóricos y normativos respecto a la atribución de responsabilidad penal frente a nuevas formas de afectación patrimonial digital.

Suárez y Rocafuerte (2024), el objetivo de su investigación es realizar el análisis comparativo de las legislaciones de España, Argentina y Ecuador en materia de delitos informáticos, específicamente en lo concerniente al phishing. La investigación delimitó como objeto de estudio los cuerpos normativos de Argentina, Ecuador y España, realizando un análisis comparado que contempló dimensiones sociales, históricas y jurídicas relacionadas con el delito informático de phishing. Esta investigación se contrapone a los resultados obtenidos en la presente investigación porque, mientras Suárez y Rocafuerte adoptan un enfoque dogmático y normativo centrado en la estructura legislativa comparada de distintos ordenamientos jurídicos frente a un tipo específico de delito (phishing), la presente investigación adopta una perspectiva penal sustantiva y procesal desde el contexto peruano, focalizándose en la imputación objetiva en el delito de fraude informático y su distinción frente a otros delitos patrimoniales como hurto, robo o estafa. Asimismo, el enfoque metodológico difiere, ya que este estudio se apoya en el análisis casuístico, jurisprudencial y en entrevistas a operadores del sistema de justicia,

mientras que el trabajo de Suárez y Rocafuerte se restringe al estudio documental y normativo comparado.

Nazario y Villanueva (2022), la investigación tiene como propósito una mejora legislativa para renovar la persecución y sanción del fraude informático en su modalidad de phishing. El análisis reveló que el artículo 8 de la Ley N° 30096 de Perú castiga los actos ilícitos cometidos mediante tecnologías informáticas en perjuicio de una o más personas, imponiendo penas de tres a ocho años de prisión y multas de entre sesenta y ciento veinte días. Sin embargo, se identificaron vacíos legales que dejan sin sanción de manera específica la modalidad de phishing. Esta investigación se contrapone a los resultados obtenidos en la presente investigación porque, mientras el enfoque de Nazario y Villanueva se centra en la insuficiencia normativa para sancionar específicamente ciertas modalidades de fraude informático como el *phishing*, el presente estudio demuestra que, más allá de las deficiencias legales, existen dificultades mayores en la aplicación práctica de la imputación objetiva en casos de fraude informático. Es decir, no se trata solamente de la tipificación normativa, sino de los retos interpretativos y procesales al momento de diferenciar estos delitos de otros patrimoniales y de determinar la responsabilidad penal concreta del imputado. Además, el presente trabajo no se limita a una propuesta legislativa, sino que analiza la jurisprudencia, casos concretos y entrevistas a operadores de justicia para evidenciar cómo se aplica realmente la ley vigente.

Tuesta (2022), tuvo como objetivo determinar cómo el fraude informático afecta los derechos fundamentales de las personas en el Cercado de Lima durante el año 2022. Los resultados revelaron que el fraude informático impacta considerablemente en los derechos fundamentales, demostrando que este delito no solo infringe derechos

específicos, sino también principios y garantías esenciales para las personas. Esta investigación se contrapone a los resultados obtenidos en la presente investigación porque, mientras Tuesta centra su análisis en las consecuencias del fraude informático desde una perspectiva de vulneración de derechos humanos, el presente estudio se orienta hacia el análisis penal del delito, específicamente en la forma en que se configura la imputación objetiva en estos casos. Es decir, la investigación actual no se enfoca en el impacto social o constitucional del delito, sino en los criterios jurídicos que permiten diferenciar el fraude informático de otros delitos patrimoniales, analizando casos concretos, jurisprudencia y opiniones especializadas para comprender cómo se estructura la responsabilidad penal del agente en el marco del derecho penal moderno.

Valdivia (2023), buscó evaluar la eficacia de las técnicas investigativas empleadas en la persecución penal del fraude informático en Perú. El estudio concluyó que las técnicas investigativas empleadas por el Ministerio Público peruano en casos de fraude informático se categorizan en: (1) actuaciones comunes como declaraciones y pericias; (2) actuaciones jurisdiccionales que requieren autorización judicial, incluyendo levantamiento del secreto de comunicaciones, acceso a información bancaria, allanamientos y geolocalización, permitiendo identificar a titulares de líneas telefónicas y cuentas bancarias, así como incautar elementos relacionados con el delito; (3) técnicas especiales como el agente encubierto, que facilita la identificación de miembros y líderes de organizaciones criminales; y (4) cooperación internacional con proveedores de internet como Google, Microsoft o Netflix para obtener información de suscriptores que pudieran estar vinculados a actividades ilícitas. Esta investigación se contrapone a los resultados obtenidos en la presente investigación porque, Valdivia se enfoca exclusivamente en la eficacia de los mecanismos de investigación criminal frente al fraude informático,

mientras que el presente estudio se centra en el análisis dogmático y jurídico de la imputación objetiva del delito, estableciendo criterios diferenciadores frente a otras figuras patrimoniales como el hurto, robo o estafa. Es decir, mientras Valdivia analiza la etapa procesal de investigación y persecución penal, esta investigación se sitúa en el plano del análisis penal sustantivo y teórico, específicamente en cómo se construye la responsabilidad penal en estos delitos dentro del marco jurídico nacional.

Según Chuco (2023), el propósito fundamental de su investigación fue examinar la relación entre el delito de fraude informático y el hurto como delito precedente, en el contexto del Cercado de Lima durante el año 2020. La investigación concluyó que el delito de fraude informático no debe ser subsumido dentro de las modalidades específicas del hurto como delito previo, ni debe considerarse dependiente o subordinado a un delito base, rechazando la premisa de que su configuración esté condicionada a la consumación previa del delito de hurto. Adicionalmente, se enfatiza la necesidad de un análisis meticuloso en cada denuncia para determinar adecuadamente la modalidad y circunstancias fácticas. Esta investigación se contrapone a los resultados obtenidos en la presente investigación porque, mientras Chuco sostiene una clara separación entre el fraude informático y el hurto, rechazando cualquier relación de subordinación o dependencia entre ambos, la presente investigación considera que es precisamente la dificultad en la delimitación entre estas figuras la que genera problemas en la aplicación de la imputación objetiva. Desde este punto de vista, el presente estudio reconoce que en muchos casos existe una superposición fáctica entre el fraude informático y ciertos delitos patrimoniales como el hurto, lo cual obliga a los operadores jurídicos a realizar una diferenciación minuciosa para evitar errores de tipificación y lograr una correcta atribución de responsabilidad penal.

Condori (2020), se llevó a cabo un estudio cuyo objetivo fue identificar las implicaciones jurídicas del fraude informático y su vínculo con la protección penal en delitos contra el patrimonio en el Distrito Fiscal de Lima Norte. El estudio concluyó que el fraude informático vinculado a delitos patrimoniales implica conductas que coinciden con otras tipificaciones de delitos patrimoniales. Aunque el fraude informático se refiere a causar un daño patrimonial mediante la alteración o manipulación de datos y software en sistemas informáticos, la investigación señaló que, a pesar de su relevancia actual, aún existe una falta de claridad metodológica que dificulta la realización de investigaciones efectivas para obtener resultados satisfactorios en estos casos. Esta investigación se contrapone a los resultados obtenidos en la presente investigación porque, mientras Condori destaca la falta de claridad metodológica como el principal obstáculo para una correcta persecución penal del fraude informático, la presente investigación evidencia avances en el uso de herramientas y técnicas especializadas (como pericias informáticas, geolocalización y cooperación interinstitucional), además de una creciente precisión conceptual en la diferenciación con otros delitos patrimoniales. Asimismo, el presente estudio sostiene que el problema actual radica más en la adecuada aplicación de la imputación objetiva y en el entrenamiento de los operadores jurídicos, que en una supuesta indefinición metodológica general.

Según Mancilla (2022), el objetivo de este estudio fue analizar la aplicación de la acusación fiscal en casos de fraude informático en el Distrito Fiscal de Lima durante el año 2022. Los resultados mostraron una aplicación inadecuada de la acusación fiscal en los casos de fraude informático en el Distrito Fiscal de Lima en 2022. Este problema se atribuye a dos factores principales: en primer lugar, la incorrecta tipificación de los delitos de fraude electrónico, que dificulta que los fiscales formulen acusaciones técnicamente

adecuadas; y en segundo lugar, la constante evolución de los sistemas digitales, que genera una innovación continua en las modalidades delictivas electrónicas, lo que hace que la normativa peruana sea insuficiente para abordar de manera efectiva estos nuevos retos. Esta investigación se contrapone a los resultados obtenidos en la presente investigación porque, mientras Mancilla señala una aplicación inadecuada de la acusación fiscal debido a una incorrecta tipificación del fraude informático y a la falta de actualización normativa frente a la evolución tecnológica, la presente investigación concluye que, si bien existen desafíos en la adaptación legal, las reformas recientes y el fortalecimiento en la capacitación de los fiscales han permitido una mejora significativa en la formulación de acusaciones. Además, se sostiene que los avances tecnológicos han sido incorporados progresivamente en el sistema penal mediante herramientas investigativas y criterios jurisprudenciales, lo que ha favorecido una mayor eficacia en la persecución del fraude informático.

García (2023), se propuso examinar la relación entre la obtención fraudulenta de créditos bancarios durante la pandemia de COVID-19 y el delito informático, bajo el marco legal vigente en 2021. La investigación concluyó que el fraude crediticio bancario carece de tipificación específica en el código penal peruano. Si bien existen normativas asociadas, como aquellas referentes a delitos contra el orden financiero y la Ley 30096 de Delitos Informáticos, estas no contemplan claramente disposiciones específicas para esta modalidad de ciberdelito, especialmente en el contexto pandémico. Consecuentemente, el estudio propone la conveniencia de desarrollar un anteproyecto legislativo que incorpore explícitamente este delito en el código penal. Esta investigación se contrapone a los resultados obtenidos en la presente investigación porque, mientras García sostiene que el fraude crediticio bancario en el contexto de la pandemia no cuenta

con una tipificación penal clara y propone la necesidad de una reforma legislativa específica, la presente investigación concluye que el marco legal vigente, particularmente la Ley N° 30096 y las disposiciones sobre delitos contra el patrimonio y el sistema financiero, permiten una adecuada interpretación y aplicación al caso del fraude informático en sus diversas modalidades, incluyendo el fraude crediticio. Asimismo, se argumenta que, a través de una interpretación sistemática y una praxis fiscal adecuada, es posible sancionar eficazmente estos delitos sin requerir necesariamente una nueva tipificación legislativa.

4.2. Limitaciones

En términos de limitaciones, solo se lograron realizar entrevistas con especialistas a nivel local, lo que impidió acceder a la perspectiva de expertos extranjeros con amplia experiencia en el campo de la criminalidad informática. Este acceso habría sido invaluable para la investigación, dado que en el Perú hay escasez de especialistas con conocimientos profundos en este ámbito.

En cuanto a la viabilidad de la investigación, la información recopilada proviene principalmente de repositorios de universidades nacionales y extranjeras, así como de noticias y sitios web internacionales. Es relevante destacar que aún en el Perú existe una falta de información complementaria que podría resolver muchas incertidumbres sobre los delitos informáticos. La mayoría de los datos fueron obtenidos de tesis internacionales, lo que subraya la escasez de material de investigación a nivel nacional.

Limitaciones de la investigación

Estas limitaciones se dividirán principalmente en dos aspectos: primero, los desafíos enfrentados en términos de posición y la viabilidad de las fuentes y recursos

económicos; y segundo, las limitaciones inherentes a la investigación, que incluyen los recursos humanos y la viabilidad de la propuesta presentada, tal como se detalla en los párrafos siguientes:

La ausencia de estudios previos y la limitada disponibilidad de fuentes bibliográficas especializadas en delitos informáticos requirieron una búsqueda exhaustiva de antecedentes y marco teórico. Se recurrió a diversas fuentes como artículos académicos, consultas en línea, opiniones de especialistas en delitos informáticos, revistas y noticias relevantes. Esta variedad de recursos fue crucial para obtener el material necesario y construir una base sólida para la investigación.

Además, se enfrentó el desafío de la falta de datos confiables y la escasez de terminología técnica adecuada en el tema. Para abordar esta carencia, se priorizó la consulta con expertos y la revisión minuciosa de literatura actualizada para asegurar la precisión y relevancia de los conceptos utilizados en el estudio. Esta combinación de métodos de búsqueda rigurosa y colaboración con especialistas permitió superar las limitaciones iniciales y establecer un fundamento sólido para la investigación sobre los estándares del delito de fraude informático en el contexto jurídico peruano.

4.3. Implicancias y estudios a futuros

Las implicancias de esta investigación se estructuran en tres dimensiones cruciales: práctica, teórica y metodológica.

Implicancia práctica

En primer lugar, desde una perspectiva práctica, este estudio busca contribuir a la mejora de la aplicación de estándares de imputación objetiva en el delito de fraude informático frente a otros delitos contra el patrimonio en lima, 2024. Esto implica

proporcionar directrices claras y efectivas para la correcta identificación y penalización de este tipo de delitos, que son cada vez más relevantes en la era digital.

Implicancia teórica

Desde un punto de vista teórico, la investigación se enfoca en enriquecer el conocimiento existente sobre el fraude informático y su distinción con otros delitos patrimoniales. Se busca profundizar en las bases conceptuales y doctrinales que sustentan la tipificación y persecución de estos delitos, proporcionando una base teórica robusta que pueda servir de referencia para futuros estudios y debates en el campo del derecho penal y las ciencias jurídicas.

Implicancia metodológica

En cuanto a la dimensión metodológica, la investigación emplea un enfoque analítico y comparativo para examinar la efectividad de la imputación objetiva y subjetiva en el fraude informático. Se utiliza una metodología rigurosa que incluye el análisis de normativas, jurisprudencia y estudios de caso, así como entrevistas con expertos legales y judiciales. Este enfoque metodológico no solo facilita la comprensión profunda del problema investigado, sino que también establece un marco claro para la evaluación crítica de las prácticas actuales y la formulación de recomendaciones concretas para mejorar la legislación y su aplicación en este ámbito específico.

4.4. Conclusiones

Primera

En relación al análisis de la aplicación de la imputación objetiva en el delito de fraude informático, frente a los delitos contra el patrimonio en Lima durante el año 2024, de evidencian múltiples dificultades tanto a nivel normativo como práctico, es decir la estructura de los delitos patrimoniales no se adecúan plenamente a las características del

delito de fraude informático, lo que genera vacíos interpretativos y desafíos en la tipificación penal, es por ello que nuestros operadores de justicia concurren en error.

Segunda

Respecto a las dificultades que enfrenta los procedimientos por robo al aplicar la imputación objetiva en los casos de fraude información, se evidenció que los procedimientos por robo enfrentan limitaciones significativas debido a que el delito de fraude informático no implica violencia ni apoderamiento físico inmediato, según lo indicado por la Ley. La incongruencia entre la mecánica del delito y los elementos típicos del robo impide una correcta calificación jurídica.

Tercera

En cuanto a las dificultades que enfrenta los procedimientos por hurto al aplicar la imputación objetiva en los casos de fraude informático, se encontró que el fraude informático no cumple con la exigencia del desapoderamiento físico y directo del bien mueble, lo que dificulta su tratamiento desde la óptica del hurto clásico. La inexistencia de contacto físico y la mediación tecnológica generan problemas para aplicar correctamente los criterios de imputación objetiva en estos casos.

Cuarto

En lo referido a las dificultades que enfrenta los procedimientos por estafa al aplicar la imputación objetiva en los casos de fraude informático, si bien existe una mayor similitud estructural con el fraude informático particularmente en cuanto al engaño y el desplazamiento patrimonial, aún persisten dificultades interpretativas. Especialmente, cuando el engaño se produce mediante sistemas automatizados o sin interacción humana directa, lo cual plantea nuevos retos en la determinación del riesgo penalmente relevante.

REFERENCIAS

Cadillo, B. (2022). *La evidencia digital en el cibercrimen - Perú 2022.* [Tesis de Pregrado, Universidad Privada del Norte]. https://repositorio.upn.edu.pe/bitstream/handle/11537/32802/Cadillo%20Quispe%2C%20Bryan%20Antonio.pdf?sequence=1&isAllowed=y

Carbajal, M. (2022). *Las fiscalías especializadas en delitos informáticos como mecanismo para la lucha contra el cibercrimen.* [Tesis de Maestría, Universidad de San Martín de Porres]. https://repositorio.usmp.edu.pe/bitstream/handle/20.500.12727/11398/carbajal_cm.pdf?sequence=1&isAllowed=y

Chiluisa, D. (2021). *Los delitos informáticos y los vacíos legales que afectan a los ciudadanos*. [Tesis de Pregrado, Universidad Católica de Santiago de Guayaquil]. http://repositorio.ucsg.edu.ec/bitstream/3317/16501/1/T-UCSG-PRE-JUR-DER-MD-334.pdf

Chuco, E. (2023). *Análisis del delito de fraude informático y hurto como delito previo, Cercado de Lima – 2020*. [Tesis de Pregrado, Universidad César Vallejo]. https://repositorio.ucv.edu.pe/handle/20.500.12692/125058

Condori, R. (2020). *Implicancias Jurídicas del Fraude Informático y la Protección Penal del Delito Contra el Patrimonio Distrito Fiscal de Lima Norte 2020.* [Tesis de Maestría, Universidad César Vallejo]. https://repositorio.ucv.edu.pe/handle/20.500.12692/63158

Corte Suprema de Justicia de la República. (2021). Sala Penal Permanente Casación. N.°

536-2020. Arequipa: 30 de septiembre de 2021. https://cdn.gacetajuridica.com.pe/laley/CASACI%C3%93N%20N%20536%202020%20AREQUIPA.pdf

Corte Suprema de Justicia de la República. (2023). Recurso Casación. N.º 2872-2022. San Martín: 21 de julio de 2023. https://www.gob.pe/institucion/pj/normas-legales/4549581-2872-2022-san-martin

Corte Suprema de Justicia de la República. (2024) Recurso Casación N.º 3330-2022. El Santa: 14 de febrero de 2024. https://www.gob.pe/institucion/pj/normas-legales/5317042-3330-2022-el-santa

Cruz, J. (2023). *Propuestas para neutralizar la alta incidencia del delito de estafa en sus diversas modalidades.* [Tesis de Maestría, Pontificia Universidad Católica del Perú]. https://tesis.pucp.edu.pe/items/01f1ec3b-166e-4ffb-a130-de67c6d54524

Cruzado, C. (2021). *Los delitos informáticos en argentina a partir de la adhesión al convenio de Budapest.* [Tesis de Maestría, Universidad Nacional de Cuyo]. https://bdigital.uncu.edu.ar/objetos_digitales/19737/cruzado-tesis-.pdf

García, P. (2023). *Obtención fraudulenta de crédito bancario como delito informático en etapa de pandemia lima, 2021.* [Tesis de Pregrado, Universidad Autónoma del Perú]. https://repositorio.autonoma.edu.pe/handle/20.500.13067/2426?show=full

Gómez, F. y Zúñiga, I. (2022). *Análisis del delito de fraude informático*. [Tesis de Pregrado, Universidad Autónoma del Chile]. https://www.studocu.com/cl/document/universidad-autonoma-de-chile/derecho-penal-i/tesis/88357272

Huamán, M. (2020). *Los delitos informáticos en Perú y la suscripción del convenio de Budapest.* [Tesis de Pregrado, Universidad Andina del Cusco]. https://repositorio.uandina.edu.pe/item/5d18fb80-74f6-49c2-80d0-0b3aba8efbd8

León, Y. (2018). *Bloqueo del IP dinamico dentro del comercio electrónico como medida de prevención de los delitos informáticos.* [Tesis de Pregrado, Universidad Señor de Sipán]. https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/5463/Le%c3%b3n%20Ochoa%20Yorli%20Adrian.pdf?sequence=1&isAllowed=y

Mancilla, S. (2022). *La acusación fiscal en el delito de fraude informático en el Distrito Fiscal de Lima 2022.* [Tesis de Pregrado, Universidad César Vallejo]. https://repositorio.ucv.edu.pe/handle/20.500.12692/113602

Mesa, M. y Ponce, L. (2023). La Regulación de los Delitos Informáticos en Colombia: Logros y Falencias en una sociedad de Cibercriminalidad en auge. *Revista XX, 20(20), 2023, 20-20.* https://repository.ces.edu.co/items/cdf67c51-8f2d-47d2-babc-0724e2560066

Ministerio Público Fiscalía de la Nación. (2022). Ministerio Público logró condena anticipada por el delito de fraude informático. https://www.gob.pe/institucion/mpfn/noticias/601113-ministerio-publico-logro-condena-anticipada-por-el-delito-de-fraude-informatico

Ministerio Público Fiscalía de la Nación. (2024). Ministerio Público logra primera sentencia por delito de fraude informático mediante el uso de criptomonedas. https://www.gob.pe/institucion/mpfn/noticias/943182-ministerio-publico-logra-primera-sentencia-por-delito-de-fraude-informatico-mediante-el-uso-de-criptomonedas

Nazario, N. y Villanueva, L. (2022). *Fraude informático en la modalidad de phishing y la necesaria actualización de la legislación para una eficiente persecución y sanción penal*. [Tesis de Pregrado, Universidad Señor de Sipán]. https:/repositorio.uss.edu.pe/handle/20.500.12802/10002

Paguay, V. (2020). *Las nuevas perspectivas regulatorias de delitos informáticos en las compras a través de internet*. [Tesis de Pregrado, Universidad Nacional de Chimborazo]. http://dspace.unach.edu.ec/bitstream/51000/7607/1/8.-TESIS%20VER%C3%93NICA%20LILIANA%20PAGUAY%20CALDER%C3%93N-DER.pdf

Poder Judicial del Perú. (2024). Corte de Lima Sur sentenció en un solo día a extranjero por fraude informático en el metro de Lima. https://www.pj.gob.pe/wps/wcm/connect/cortesuperiorlimasurpj/s_csj_lima_sur_nuevo/as_inicio/as_imagen_prensa/as_noticias/csjls_n_np_00011_2024#:~:text=Sonia%20Quispe%20Silva%2C%20conden%C3%B3%20a,car%C3%A1cter%20suspendida%20por%20el%20periodo

Ramos, M. (2022). *Impacto de los delitos informáticos en las investigaciones preparatorias de las fiscalías provinciales penales corporativas distrito fiscal Lima Sur 2022*. [Tesis de Pregrado, Universidad Norbert Wiener]. https://repositorio.uwiener.edu.pe/bitstream/handle/20.500.13053/8051/T061_73813479_TSP.pdf?sequence=1&isAllowed=y

Riega, Y.; Huamani, H. y Machuca, J. (2021). Contratación electrónica y los delitos informáticos. En protección al consumidor en el Perú. *Revista LEX*. 19, 197 - 236 https://vlex.bibliotecaupn.elogim.com//account/login_ip#/search/jurisdiction:PE+content_type:4/Contrataci%C3%B3n+electr%C3%B3nica+y+los+delitos+inform%C3%A1ticos.+En+protecci%C3%B3n+al+consumidor+en+el+Per%C3%BA/vid/contratacion-electronica-delitos-informaticos-897826669

Smith, J. (2018). "Fraude Informático: Amenazas y Desafíos en la Era Digital". *Revista Internacional de Seguridad Cibernética*, 10(2), 45-58. https://revistaderechopenal.pe/articulo/delitos-informaticos-codigo-penal-peruano

Tomillo, J. (2021). Los consumidores ante las plataformas de intermediación Online. Algunas reflexiones. *Revista LEX*, 19(27), 97 – 132. https://vlex.bibliotecaupn.elogim.com//account/login_ip#/search/jurisdiction:PE+content_type:4/Los+consumidores+ante+las+plataformas+de+intermediaci%C3%B3n+Online%3A+algunas+reflexiones/vid/consumidores-plataformas-intermediacion-online-873361778

Tribunal Constitucional. (2020). Pleno. Sentencia 1100/2020 . N.° 01189-2019-PHC/TC. Lima: 10 de diciembre de 2020. https://tc.gob.pe/jurisprudencia/2020/01189-2019-HC.pdf

Tuesta, R. (2022). *Fraude informático y su impacto en los derechos fundamentales de la persona en el Cercado de Lima – 2022*. [Tesis de Pregrado, Universidad Norbert Wiener]. https://repositorio.uwiener.edu.pe/handle/20.500.13053/8054

Valdivia, J. (2023). *La eficacia de la persecución penal del delito de fraude informático en el Perú.* [Tesis de Pregrado, Universidad Tecnológica del Perú]. https://repositorio.utp.edu.pe/handle/20.500.12867/7386

Velita, A. (2021). *Problemas de la valoración fiscal en la etapa de investigación preliminar de los delitos de fraude informático*. [Tesis de Pregrado, Universidad de San Martín de Porres]. https://repositorio.usmp.edu.pe/handle/20.500.12727/9505

ANEXOS

Anexo 1. Matrix de consistencia.

<table>
<tr><td colspan="5">Título: Imputación objetiva en el delito de fraude informático frente a los delitos contra el patrimonio en Lima 2024.</td></tr>
<tr><td colspan="2">Problemas</td><td>Objetivos</td><td colspan="2">Categorías y sub categorías</td></tr>
<tr><td colspan="2">Problema General:</td><td>Objetivo general:</td><td colspan="2">Categoría 1: Imputación objetiva en el delito de fraude informático</td></tr>
<tr><td colspan="2" rowspan="2">¿Cómo se aplica la imputación objetiva en el delito de fraude informático frente a los delitos contra el patrimonio en Lima, 2024?</td><td rowspan="2">Analizar la aplicación de la imputación objetiva en el delito de fraude informático frente a los delitos contra el patrimonio en Lima, 2024.</td><td>Sub categorías</td><td>Instrumento</td></tr>
<tr><td>− Elementos constitutivos del fraude informático
− Aplicación de la imputación objetiva en casos de fraude informático</td><td>- Guía de entrevista
- Análisis documental</td></tr>
<tr><td colspan="2">Problemas Específicos</td><td>Objetivos específicos</td><td colspan="2">Categoría 2: Delitos contra el patrimonio en Lima, 2024.</td></tr>
<tr><td colspan="2">(a) ¿Cuáles son las principales dificultades que enfrenta los procedimientos por robo al aplicar la imputación objetiva en los casos de fraude informático?
(b) ¿Cuáles son las principales dificultades que enfrenta los procedimientos por hurto al aplicar la imputación objetiva en los casos de fraude informático?
(c) ¿Cuáles son las Identificar las principales dificultades que enfrenta los procedimientos por estafa al aplicar la imputación objetiva en los casos de fraude informático?</td><td>(a) Identificar las principales dificultades que enfrenta los procedimientos por robo al aplicar la imputación objetiva en los casos de fraude informático.
(b) Identificar las principales dificultades que enfrenta los procedimientos por hurto al aplicar la imputación objetiva en los casos de fraude informático.
(c) Identificar las principales dificultades que enfrenta los procedimientos por estafa al aplicar la imputación objetiva en los casos de fraude informático.</td><td>Sub categorías</td><td>Instrumento</td></tr>
<tr><td colspan="2"></td><td></td><td>− Delito de robo
− Delito de hurto
− Delito de estafa</td><td>- Guía de entrevista
- Análisis documental</td></tr>
<tr><td>Diseño de investigación:</td><td>Escenario de estudio y Participantes:</td><td colspan="3">Técnicas e instrumentos:</td></tr>
<tr><td>− Enfoque: Cualitativo
− Tipo: Básica
− Diseño: Fenomenológico y descriptivo.</td><td>− Escenario de estudio: Lima Metropolitana
− Participantes: 05 especialistas del tema</td><td colspan="3">Técnicas: Análisis casuístico, Análisis Jurisprudencial y entrevistas.
Instrumentos: Guía de entrevista y Análisis documental.</td></tr>
</table>

Anexo 2. Ficha de análisis documental.

FUENTE JURISPRUDENCIAL	CONTENIDO DE LA FUENTE JURISPRUDENCIAL	ANÁLISIS DEL CONTENIDO DE LA FUENTE JURISPRUDENCIAL	CONCLUSIÓN
Sentencia del Tribunal Constitucional del Perú, específicamente la Sentencia del Pleno del Tribunal Constitucional del 10 de diciembre de 2020, en el Expediente 01189-2019-PHC/TC.	En la sesión del Pleno del Tribunal Constitucional del 10 de diciembre de 2020, se emitió la sentencia que declaró INFUNDADA la demanda de hábeas corpus presentada por don William Renardino García Rosales a favor de Marcos Morales Vargas. La demanda cuestionaba la legalidad de una condena por fraude informático y falsificación de firma en documento privado, argumentando la aplicación retroactiva de la Ley 30096.	La sentencia analiza la aplicación del principio de legalidad penal, destacando que la Ley 30096, que sanciona el fraude informático, estaba vigente al momento de los hechos delictivos. Se discute la interpretación de los elementos constitutivos del delito y la adecuación de la norma aplicada por los tribunales ordinarios.	El Tribunal Constitucional concluyó que no hubo vulneración del principio de legalidad penal en el proceso seguido contra Marcos Morales Vargas. La sentencia destaca la importancia de la aplicación correcta de la normativa vigente al momento de los hechos para garantizar el debido proceso y la tutela judicial efectiva.

Nota. Elaboración propia.

Anexo 3. Guía de Entrevista

GUÍA DE ENTREVISTA

OBJETIVO GENERAL

Analizar la aplicación de la imputación objetiva en el delito de fraude informático frente a los delitos contra el patrimonio en Lima, 2024.

Preguntas:

De acuerdo con su experiencia

1. ¿Cuáles son los estándares de imputación objetiva que deben establecerse en la determinación del delito de fraude informático?
2. ¿Cuáles cree que son los desafíos que se enfrentan al procesar casos de fraude informático en comparación con otros delitos patrimoniales?
3. ¿Cuáles son los elementos típicos (subjetivos y objetivos) del delito de fraude informático en su discriminación con los delitos patrimoniales?

OBJETIVO ESPECÍFICO 1

Identificar las principales dificultades que enfrenta los procedimientos por robo al aplicar la imputación objetiva en los casos de fraude informático.

Preguntas:

De acuerdo con su experiencia

1. ¿Cómo se diferencia legalmente el fraude informático de otras figuras delictivas relacionadas, como el robo?
2. ¿Cuáles son las principales dificultades que enfrenta la aplicación de la imputación objetiva en los procedimientos por robo en casos de fraude informático?

OBJETIVO ESPECÍFICO 2

Identificar las principales dificultades que enfrentan los procedimientos por hurto al aplicar la imputación objetiva en los casos de fraude informático.

Preguntas:

De acuerdo con su experiencia

1. ¿Cómo se diferencia legalmente el fraude informático de otras figuras delictivas relacionadas, como el hurto?
2. ¿Cuál es su opinión sobre la legislación peruana actual frente a los delitos de fraude informático en discriminación con el delito de hurto?

OBJETIVO ESPECÍFICO 3

Identificar las principales dificultades que enfrentan los procedimientos por estafa al aplicar la imputación objetiva en los casos de fraude informático.

Preguntas:

De acuerdo con su experiencia

1. ¿Cómo debería construirse la imputación en casos de pluralidad de agentes en el delito de fraude informático vinculada en delitos de estafa?
2. ¿Cuáles son las principales dificultades que enfrentan los órganos jurisdiccionales al procesar casos de fraude informático en comparación con en el delito de estafa