UNIVERSIDAD DE PANAMÁ

VICERRECTORÍA DE INVESTIGACIÓN Y POSTGRADO

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

“ESTAFA A TRAVÉS DE MEDIOS INFORMÁTICOS EN PANAMÁ”

TESIS DE GRADO PARA OPTAR POR EL TÍTULO DE MAGISTER EN DERECHO

CON ÉNFASIS EN DERECHO PENAL

OLMEDO ENRIQUE GOMEZ MORA

ASESORA

DRA. VIRGINIA ARANGO DURLING

2026

ÍNDICE

INTRODUCCIÓN

En la era digital actual, la tecnología se ha consolidado como una herramienta indispensable en la vida cotidiana de todas las personas, transformando la manera en que interactúan, trabajan y gestionan sus actividades diarias. Sin embargo, junto con los beneficios asociados a la digitalización, emergen nuevos desafíos que impactan la seguridad jurídica, económica y social de los individuos y las instituciones.

Ante esta realidad, subyace un fenómeno mediante el aumento de los delitos informáticos, especialmente la estafa a través de medios informáticos. Este delito ha experimentado un crecimiento vertiginoso en los últimos años a nivel mundial, y en particular en la República de Panamá. Este acontecimiento delictivo ha evidenciado las limitaciones de las normativas vigentes para responder de manera efectiva a las nuevas modalidades delictivas.

De acuerdo con lo expuesto, es importante destacar que la legislación penal en diferentes países, incluido Panamá, aún no cuenta con un marco legal específico que regule de manera autónoma y clara las conductas relacionadas con la estafa a través de medios tecnológicos. En la actualidad, la mayoría de las normas existentes regulan la estafa y otros fraudes de forma general, lo que puede dificultar su correcta interpretación y aplicación, especialmente en aquellos casos en los que se encuentran vinculados con nuevas tecnologías.

Por consiguiente, esta situación genera problemas de impunidad y además limita la protección efectiva de las víctimas, quienes en estos casos suelen ser usuarios o consumidores de servicios digitales vulnerables a diversos engaños y fraudes. En este contexto, esta problemática evidencia que la estafa a través de medios informáticos presenta características propias que la diferencian claramente de la estafa tradicional.

Entre estas características se destacan el uso de artificios tecnológicos, la manipulación de datos, la creación de sitios web falsos y el envío de correos fraudulentos, entre otros. Los mecanismos mencionados anteriormente facilitan que los delincuentes actúen con rapidez y ambigüedad, por tanto, la ausencia de una figura penal específica para estos delitos en la legislación panameña evidencia una gran dificultad tanto en la persecución y sanción de los mismos, siendo imprescindible el establecimiento de un marco normativo actualizado que facilite la tipificación y sanción efectiva de los delitos de estafa en el entorno digital.

El presente trabajo tiene como finalidad analizar la situación actual de la estafa a través de medios informáticos en Panamá, identificando las principales modalidades que adoptan estas conductas y comprender sus particularidades, con el fin de destacar las dificultades que enfrentan las autoridades judiciales ante un marco legal que resulta insuficiente para garantizar la protección de los bienes jurídicos afectados, también se abordará la experiencia comparada de otros países que han establecido tipos penales específicos para estos delitos, para proponer una legislación que se ajuste a las características propias de la criminalidad digital.

El presente trabajo estará comprendido por los siguientes capítulos:

- Capitulo I. Aspectos generales de la investigación
- Capitulo II. Marco Teórico
- Capítulo III. Análisis dogmático del delito de Estafa a través de medios informáticos en Panamá.
- Capítulo IV. Estafa Informática en el derecho comparado desde la regulación y necesidad de un tipo especial en Panamá.
- Conclusiones y recomendaciones.

CAPITULO I. ASPECTOS GENERALES DE LA INVESTIGACIÓN

1.1. Planteamiento del problema

Latinoamérica ha experimentado recientemente un aumento significativo de la frecuencia y sofisticación de los ciberataques. Los sectores afectados incluyen la administración pública, las finanzas, la energía y las infraestructuras críticas, así como a particulares y empresas. La región se caracteriza por una carencia de medidas de seguridad efectivas, una baja conciencia en ciberseguridad y el uso de tecnologías insuficientemente seguras (Rendón et al., 2024).

Por ende, el uso creciente de las tecnologías digitales en el sector bancario ha provocado un fuerte aumento de los intentos de fraude digital, específicamente en los servicios de banca online. Este tipo de fraude se ha convertido en un problema global y ha transformado a este sector en un terreno fértil para los ciberdelincuentes que utilizan métodos sofisticados como ataques de phishing, ataques de denegación de servicio, troyanos, software malicioso, robo de identidad y virus informáticos (Ahmad et al., 2024).

Esta situación ha alcanzado a niveles críticos de ciberataques en la sociedad de Latinoamericana, así lo establece el Registro de Direcciones de Internet de América Latina y Caribe (LACNIC) (2018) mencionando que el phishing estuvo en el año 2018 como una de las principales amenazas en la sociedad latinoamericana sobresaliendo con el 60% y adquiriendo entre el 15% y 20% de las economías que el internet genera por año.

Por lo que respecta a Panamá, la estafa informática o por medios informáticos está prevista en el artículo 226 acentuando que se castigarán la realizadas a través de la manipulación de bases de datos y sistemas informáticos. Este hecho pone en una situación problemática a este país, debido a la falta de un tipo penal específico que castigue este tipo de criminalidad que cada año va en aumento.

Una investigación realizada por Guzmán et al. (2023) concluyó que en Panamá los ciberdelitos es una problemática que van en ascenso, específicamente en la provincia de Panamá ya que cuenta con una incidencia de

- 29.95 por cada 100,000 habitantes durante los años 2019-2020
- 49.64 por cada 100,000 habitantes durante los años 2020-2021
- 35.76 por cada 100,000 habitantes durante los años 2021-2022

Siendo los ciberdelitos más frecuentes los fraudes, la venta y divulgación de contenido sin permiso, el phishing, el intrusismo y extorción. Por ende, esta situación es un problema crítico porque la estafa por medios informáticos es un hecho que, si bien tiene cualidades comunes con la estafa tradicional, el beneficio para el sujeto activo y perjuicio económico ilícito al sujeto pasivo son totalmente diferentes.

En la estafa tradicional, persiste el engaño directo y presencial, mientras que en la estafa informática ocurre mediante artificios o manipulación de sistemas informáticos cuando introducen datos falsos o crean datos que simulen una realidad

falsa, lo cual provoca un engaño mediante una comunicación electrónica. Ante este estas circunstancias, se manifiesta el requerimiento de una respuesta legal eficiente.

Por ende, se tiene la necesidad de identificar las particularidades de la estafa Informática a fin de justificar la necesidad político-criminal de su inserción en la legislación penal como delito especifico, a fin de adecuar dicha legislación a los avances tecnológicos, ya que esto permitirá que la ciudadanía y en particular a la administración de justicia tener una mayor formación en delitos informáticos o cibernéticos, permitiéndoles ejercer una persecución penal más eficaz evitando la impunidad.

1.2. Antecedentes

La estafa a través de medios cibernéticos o informáticos es un tema de relevancia en la actualidad por el creciente aumento de actividades delictivas en el ciberespacio. La estafa informática es un delito contra el patrimonio económico que consiste en la manipulación informática, un hecho en la que se hace uso ilegitimo de medios tecnológicos y de comunicación que incluye el uso de internet, correos electrónicos, sitios web falsos y otros medios digitales (FTC, 2022).

La manipulación informática implica actuación incorrecta del sujeto activo sobre un sistema informático de manera que modifique el resultado de un procesamiento automatizado en cualquiera de las fases de procesamiento o tratamiento informático con ánimo de lucro y perjuicio a un tercero (Faraldo Cabana, 2007).

Los antecedentes de los delitos informáticos se remontan a los primeros días de la informática y de internet, cuando las computadoras comenzaron a conectarse en redes, y esto creó nuevas oportunidades para diversificar las formas de materializar acciones delictivas derivadas de estas innovaciones, dando lugar a las primeras expresiones de estafa a través del uso de medios cibernéticos, lo cual a través del tiempo ha ido evolucionando (Del Pino, 2016). A principios de la década de los 70, la comisión de acciones delictivas era proferida vía telefónica, y las personas que cometían estas acciones en principio, se les denominó Phreakers, que eran hackers que tuvieron una finalidad maliciosa.

Suárez Sánchez (2007) describe que ante la notoriedad del aumento de fraudes a través de la manipulación de tarjetas de débito en cajeros automáticos y la vulneración de bandas magnéticas, comienza el desarrollo de una protección normativa en Estados Unidos (1978), y se promulga una ley en 1986 para sancionar el abuso y fraude informático.

Seguidamente, en el 2001 inicia el Convenio sobre la ciberdelincuencia siendo el primer tratado internacional que regula los delitos cometidos en el ciber espacio, teniendo como finalidad brindar estándares en materia de derecho penal y desarrollar procedimientos adecuados en el entorno digital, de esta manera, establecer los mecanismos donde se establecen la cooperación internacional en materia de cibercriminalidad, ratificado por Panamá mediante la Ley 79 de 22 de octubre de 2013.

Por lo que respecta a Panamá, el Código Penal de 2007 aborda la Estafa y otros fraudes en los artículos 200 a 226 y en el artículo 226 específicamente contempla las estafas realizadas a través de la manipulación de bases de datos y sistemas informáticos y no como un delito autónomo, lo que trae dificultades para su comprensión y aplicación legal, ya que la estafa Informática requiere de un estudio y abordaje de manera específica, es decir, como un delito informático para que la administración de justicia tenga instrumentos efectivos para enfrentar adecuadamente este tipo de criminalidad, así lo han previsto otros países como España.

El Código Penal Español en los artículos 248.2 y 248.3 establece que “son reos de estafa los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio similar, logren la transferencia no consentida de cualquier activo patrimonial”. (Naciones Unidas, 2015). Esto implica que se sanciona al poseedor del instrumento o medio a través del cual se comete el delito, como en el caso de una computadora. Además, se establece que “la misma pena se aplicará a quienes fabriquen, introduzcan, posean o faciliten programas de ordenador específicamente destinados a la comisión de las estafas previstas en este artículo” (Naciones Unidas, 2015).

Por tanto, se requiere de un tipo penal de estafa informática individualizado porque es necesario tomar en cuenta la variedad de tipologías, tales como Pharming,

Spim, Phishing y Smishing, que se han consolidado con el avance de las tecnologías de la información a efectos de evitar la impunidad y adoptar medidas preventivas.

Por otro lado, al examinar los recursos bibliográficos sobre la estafa por medios informáticos se detectó una carencia bibliográfica sobre el tema en Panamá, dado que la mayoría de los estudios se concentran en la estafa tradicional o aislada de las que involucra tecnologías digitales. Esta falta de atención específica destaca que muchos de los investigadores no han enfocado sus análisis en este fenómeno particular, el cual merece ser examinado y explicado con mayor detalle.

1.3. Objetivos

1.3.1. Objetivo General

Analizar el delito de Estafa Informática en Panamá en su regulación vigente.

1.3.2. Específicos

- Investigar sobre la Estafa informática como delito autónomo en Panamá.
- Determinar las tipologías más comunes de la Estada informática.
- Identificar, las razones que justifican desde una política criminal la inclusión autónoma de la Estafa Informática en la legislación panameña.

1.4. Justificación

El motivo del estudio sobre la estafa a través de medios informáticos surge en el contexto del creciente avance y uso de la tecnología en Panamá, lo que ha facilitado un aumento alarmante en las estafas informáticas. Este fenómeno representa un desafío importante para la seguridad personal y financiera de los

ciudadanos panameños, lo que resalta la necesidad urgente de abordar la problemática desde una perspectiva penal, sin dejar de lado las medidas preventivas recomendadas para reducir estos riesgos.

En virtud de lo mencionado, resulta fundamental conocer, comprender y proporcionar información sobre la estafa informática, ya que los estudios actuales en Panamá se han centrado solo en el análisis e interpretación de la estafa convencional o tradicional, desestimando que los medios electrónicos en la estafa Informática ofrecen nuevas posibilidades delictivas por las diversas tipologías o formas de realizarse, lo que provocan graves perjuicios económicos ante una nueva versión delictiva que tiene elementos especiales y se realiza con la mayor agilidad y rapidez.

En efecto, las tipologías más frecuentes de estafa informática comprenden: Pishing, Pharming,Carding,Vishing o Smishing, de los cuales en Panamá durante el período 2019-2022 se han detectado el fraude o estafa, la difusión de contenido íntimo, el phishing, el intrusismo y la extorsión. Por ende, para dar conformidad al trabajo se hace necesario estudiar sobre la estafa informática y proponer un modelo de tipo penal que sea más acorde con la actualidad informática con el propósito de:

- Garantizar la seguridad jurídica
- Facilitar la persecución penal y evitar la impunidad de estos hechos
- Dar cumplimiento al Convenio sobre Ciberdelincuencia de 2001.

1.5. Hipótesis

La ausencia de un tipo autónomo de la estafa Informática dificulta determinar cuándo se concreta este fenómeno delictivo, su persecución penal, promueve la inseguridad jurídica, y conduce a la impunidad.

CAPITULO II- MARCO TEÓRICO

2.1. Origen y evolución de la Estafa a través de medios informáticos.

2.1.1. Introducción

Las conductas más perniciosas que atentan contra el patrimonio de los individuos se encuentran aquellas que se valen del engaño como mecanismo para despojar a los particulares de sus bienes. Estas modalidades delictivas caracterizadas por su naturaleza fraudulenta, representan una amenaza significativa para la integridad patrimonial y para la confianza en las relaciones económicas, lo cual justifica un análisis pormenorizado de su configuración jurídica y sus implicaciones en el ámbito del derecho penal (Muñoz, 2008).

Aunado a ello, es pertinente subrayar que la transición hacia una sociedad de libre mercado y el desarrollo de tecnologías que facilitan la intermediación en los medios de comunicación han propiciado nuevas posibilidades de aprovechamiento indebido e ilícito. Esta dinámica, observada desde una óptica evolutiva, remonta sus orígenes a la invención del telégrafo y del teléfono y se ha incorporado progresivamente en la vida cotidiana de las personas.

Actualmente se debe partir del hecho de que un ordenador, teléfono móvil o cualquier otro dispositivo tecnológico puede almacenar y archivar todo tipo de datos.

En las últimas décadas, la calidad, el volumen y el valor de la información conservada en dichos dispositivos han crecido de forma exponencial, constituyéndose en un símbolo de racionalidad y progreso. No obstante, esos sistemas informáticos pueden también ponerse al servicio del crimen, lo que plantea nuevos desafíos en materia de seguridad y protección jurídica.

La criminalidad a través de medios informáticos ha dejado de limitarse a conductas asociadas a dispositivos concretos (ordenadores, teléfonos, correos electrónicos) y se vincula actualmente con los medios de comunicación y herramientas tecnológicas contemporáneas entre ellas, la inteligencia artificial (Veloz et al., 2026). Esta realidad obliga a la administración de justicia a mantenerse a la vanguardia frente a un delincuente que con frecuencia, se anticipa a la legislación y dificulta la protección efectiva de los bienes jurídicos.

2.1.2. Orígenes y antecedentes

En cuanto a los orígenes de este fenómeno, cabe señalar que la estafa a través de medios informáticos denominada por la doctrina como ciberestafa o fraude en línea, encuentra sus raíces en la evolución tecnológica y el auge de internet. Es importante acotar que, la estafa no es un delito menor y que la estafa informática se ha perfeccionado a medida que las computadoras y la conexión a la red se convirtieron en medios de comunicación e intercambio de información accesibles para el público, especialmente desde mediados de la década de 1980 hasta principios de los años 90, los delincuentes comenzaron a identificar el potencial de estas herramientas para cometer fraudes. Este contexto histórico marca el inicio de

una nueva modalidad delictiva que se ha ido sofisticando con el avance de la tecnología (Miró, 2011).

Uno de los primeros tipos de estada informática fue el famoso timo del *príncipe nigeriano* que surge a mediados de los 90, consistía en enviar correos electrónicos masivos solicitando ayuda para transferir grandes sumas de dinero, prometiendo una generosa recompensa a cambio. Aunque esto parezca poco creíble, muchas personas cayeron en este engaño marcando un inicio de una nueva era de Estafas en línea. (Estwood, 2025).

Con el paso del tiempo y el desarrollo de nuevas tecnologías ha evolucionado a lo que se ha convertido el phishing, siendo este una técnica que implica suplantar la identidad legitima para obtener información confidencial, se hizo popular a principio de los años 2000, donde los estafadores creaban sitios web que imitaban a los bancos o servicios en línea populares para engañar a los usuarios y robar sus datos (Zamora Acevedo, 2025).

Para precisar la tipología delictiva antes mencionada, cabe señalar que este tipo de conductas comenzó a desarrollarse en la década de 1990, cuando se obtuvieron cuentas de la compañía AOL mediante el uso de números de tarjetas de crédito válidos, generados a través de algoritmos.

Posteriormente, con la generalización de MSN, este tipo de prácticas fraudulentas proliferaron en dicha plataforma de servicios de internet. En años más

recientes, en los servicios ofrecidos por Microsoft han surgido sitios web que, a cambio de proporcionar información sobre contactos eliminados en sus servicios de mensajería instantánea, usurpan el nombre de usuario y la contraseña de MSN (Sánchez Bernal, 2009).

A partir de aquí, en el año 2010 se abrió una nueva vía para los ciberdelincuentes a través de las conocidas redes sociales. De ello empiezan a surgir las estafas románticas. En este caso particular, los estafadores se hacen pasar por personas atractivas para manipular emocionalmente a sus víctimas con el objetivo de obtener dinero (Comisión Federal del Comercio, 2022).

En la actualidad, las estafas han alcanzado niveles de sofisticación sin precedentes a medida que los delincuentes se adaptan rápidamente a las nuevas tecnologías. Un claro ejemplo de ello es el *ransomware*, un tipo de malware que secuestra los datos de las víctimas exigiendo un rescate. Asimismo, las estafas relacionadas con criptomonedas han proliferado, aprovechando el desconocimiento de muchos usuarios sobre estos nuevos sistemas financieros digitales (Ávila-Niño, 2023).

Estos casos evidencian cómo los delincuentes están aprovechando el constante avance tecnológico para diseñar nuevas modalidades delictivas ligadas de manera intrínseca a la expansión de la tecnología. Lo que comenzó como simple fraude por correo electrónico ha evolucionado hasta convertirse en una amenaza global que requiere una vigilancia y educación constante por parte de los usuarios de

tecnología en todo el mundo. Es fundamental comprender que el desarrollo tecnológico, si bien ha traído innumerables beneficios a la sociedad, también ha sido aprovechado por grupos delictivos para cometer estafas cada vez más sofisticadas y difíciles de detectar.

2.2. La estafa informática concepto y antecedentes

Desde el inicio del siglo XXI, Panamá ha vivido un notable incremento en la adopción de tecnologías de la información y la comunicación. Esta evolución ha propiciado el surgimiento de nuevas modalidades de estafa, las cuales utilizan como herramienta principal estas tecnologías. No obstante, es importante indicar que el Código Penal panameño vigente antes de la reforma de 2007, es decir, el Código de 1982 contemplaba un concepto de estafa tradicional que no abarcaba las modalidades delictivas que ya se estaban desarrollando en el país (Godoy, 2020).

El surgimiento de este fenómeno criminal se remonta a las décadas de 1960 y 1980, cuando se comenzó a registrar su proliferación en los países más desarrollados, impulsada por la expansión de las nuevas tecnologías en las administraciones públicas y grandes empresas (Galán Muñoz, 2003). En este contexto, Panamá no es ajeno a esta realidad, ya que en ese periodo se empezaron a perfeccionar delitos de estafa que empleaban las nuevas tecnologías de la información como medio.

Para ilustrar este aspecto, conviene considerar la sentencia de casación proferida por el magistrado ponente José Ayú Prado Canals, de fecha 17 de mayo

del año 2019. Según la resolución, entre el 8 y el 9 de agosto del año 2006 los acusados mediante correos electrónicos fraudulentos, obtuvieron indebidamente información personal de varios cuentahabientes sin su consentimiento. Con base a dicha información, sustrajeron sumas significativas de las cuentas de ahorro de las víctimas, causándoles un perjuicio patrimonial (Chavarría Mendoza, 2019).

Cabe precisar que esta causa penal se originó en 2006, es decir, antes de la entrada en vigor de la Ley 79 de 2013 norma que posibilitó la aplicación del Convenio de Budapest sobre ciberdelincuencia; por tanto, el proceso se tramita bajo el amparo del Código Penal de 1982. En consecuencia, el tratamiento jurídico que le brindó el tribunal es que no fuera como estafa mediante un medio informático, sino en virtud del artículo 393-A que, a la luz del Código Penal vigente en esa época lo tipificaba como un delito financiero, de conformidad con Ley N° 45 de 4 de junio de 2003, publicada en la Gaceta Oficial N° 24.818 de 9 de junio del 2003, aplicable en el Capítulo VII. Delitos financieros (2003) en el artículo 393-A:

> Quien en beneficio propio o de un tercero, mediante la utilización de medios tecnológicos u otras maniobras fraudulentas, se apodere, haga uso indebido u ocasione la transferencia ilícita de los dineros, valores, bienes u otros recursos financieros de una entidad bancaria, empresa financiera u otra que capte o intermedie con recursos financieros del público o que le hayan sido confiados a ésta, será sancionado con presión de 3 a 5 años. La sanción será de 6 a 10 años de prisión, cuando el ilícito sea cometido por o con la participación de un

empleado, director, dignatario, administrador o representante legal de la entidad o empresa, aprovechándose de su posición o del error ajeno. (p.6)

Del artículo transcrito, corresponde históricamente analizar dos expresiones que, a la luz de la normativa vigente, difieren sustancialmente en cuanto a su tipificación y a su eficacia para sustentar un juicio de reproche. La norma alude a la utilización de medios tecnológicos u otras maniobras fraudulentas; sin embargo, no ofrece una conceptualización normativa ni una tipología clara del fenómeno delictivo al que se enfrenta, lo cual evidenciaba en aquel momento un serio desfase respecto de la realidad tecnológica.

A razón de este análisis, se apunta a que la redacción de la exerta legal examinada no distingue con claridad entre el medio (tecnológico) y la conducta típica (fraude, estafa, apropiación), lo que puede generar incertidumbre probatoria y problemas para calibrar la culpa o dolo.

En virtud de lo anterior, desde una perspectiva histórica del fenómeno criminal objeto de examen, en aquel momento no existía una tipificación clara de los conceptos involucrados. La Corte orientó correctamente la calificación del comportamiento: el medio de ejecución del ilícito se perfecciona mediante el engaño cometido con el auxilio de un elemento tecnológico; no obstante, en el delito financiero lo esencial es el acto material de sustracción, circunstancia que actualmente se encuentra adecuadamente definida en la normativa vigente.

En continuidad con la línea histórica, para el año 2007 se implementó una reforma al Código Penal de 1982 introduciendo importantes innovaciones en el ámbito del derecho penal. Estas modificaciones abarcaron tanto las figuras delictivas como la parte general del código. Destaca, por ejemplo, la inclusión de la autoría mediata, así como un enfoque renovado sobre el dolo y la culpa, que ya no se consideran meras formas de culpabilidad. Esta reforma se alinea con el Sistema Finalista del delito, orientando la interpretación y aplicación de la ley penal (Guerra de Villalaz, 2013).

La reciente modificación del Código Penal 2007 introdujo un agravante relacionado con el uso de medios informáticos, consideración que no estaba presente en el artículo 190 del Código Penal de 1982. Sin embargo, la legislación aún no tipificaba de manera explícita el fenómeno criminal bajo estudio, dejando la responsabilidad por el fraude electrónico parcialmente desatendida. Esta situación se corrigió en 2012, cuando se aprobó la Ley 51 que introdujo disposiciones más claras sobre el uso de tecnologías en el engaño y la apropiación de recursos.

Con base a lo expuesto en el párrafo anterior, el artículo 220 del Código Penal de Panamá configura la estafa informática como un ilícito consistente en provocar un perjuicio patrimonial a la víctima mediante un engaño ejecutado por medios informáticos o cibernéticos. A tal efecto, el término cibernético se entiende como aquello creado y gestionado a través de sistemas informáticos. En consecuencia, el rasgo distintivo entre la estafa tradicional y la estafa informática es el empleo de tecnologías de la información y la comunicación, por ejemplo ordenadores,

dispositivos móviles o plataformas digitales como medio instrumental para la comisión del fraude, modalidad que se manifiesta especialmente en el ámbito del comercio electrónico (Arenas, 2021).

Como conclusión de este apartado histórico, puede sostenerse que la tipificación penal vigente en Panamá resulta insuficiente frente a las actuales tipologías y conductas generadoras de estafa. De ello se deriva la necesidad de examinar sistemáticamente los distintos supuestos delictivos relacionados con los medios de pago y en particular, de distinguir entre:

- Los casos en que el medio de pago constituye el objeto material del delito por ejemplo, la clonación de tarjetas, la falsificación, el tráfico y el apoderamiento ilícito de datos
- Aquellos supuestos en que el medio de pago opera como instrumento para la comisión de un delito, mediante su uso ilícito (o el uso indebido de los datos asociados), culminando en la disposición patrimonial indebida de los fondos (Carrillo, 2013).

La problemática relacionada con el delito de estafa se centra en que su definición clásica establece que el autor del engaño debe ser una persona física y que el acto engañoso debe ser lo suficientemente relevante como para provocar un error en la víctima, lo que a su vez desencadena una alteración en su situación patrimonial.

Esta perspectiva se apoya en una reciente sentencia del Tribunal Supremo Español, que sostiene que no se puede considerar como estafa el pago realizado con una tarjeta que no pertenece al comprador, cuando este presentó su documento de identidad durante la transacción.

El razonamiento expuesto, apunta que no se puede hablar de engaño en este caso, ya que una actuación diligente por parte del vendedor al cumplir con sus obligaciones de verificación, habría revelado que la información del documento de identidad presentado no coincidía con la del verdadero titular de la tarjeta. Esto, a su vez, habría evitado la realización de la venta (Sánchez, 2000). En este contexto, la aplicación del derecho enfrenta retos ante las nuevas tipologías delictivas derivadas de las tecnologías de la información.

En este sentido, países como España, en 1995, incorporaron el concepto de estafa informática, en el cual se sustituyó el término tradicional engaño por la noción de manipulación informática, con el fin de adecuar la tipificación penal a las particularidades propias de las conductas delictivas desarrolladas mediante medios tecnológicos y algoritmos digitales (Polaino, 2017). Esta situación facilitó avances en la materia y propició un mayor desarrollo en el procesamiento de los tipos penales relacionados.

Para ilustrar y respaldar lo expuesto, a continuación se presenta un extracto de una sentencia del Tribunal Superior de España en materia de Estafa informática del artículo 248.2 del código penal del año 2001 y establece que “también se

consideran reos de estafa los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo" (Pérez, 2025, p.29).

A raíz de lo expuesto, se tiene que el razonamiento jurídico del tribunal se encuentra en concordancia con una normativa que intenta ajustarse a las dinámicas delictivas contemporáneas, teniendo en cuenta las modalidades y particularidades de las conductas ilícitas en su contexto actual. Sin embargo, estas consideraciones no están adecuadamente desarrolladas en la normativa penal vigente en la República de Panamá.

Tabla 1. Cuadro comparativo histórico

Cuadro Comparativo Histórico.		
Código Penal 2007	**Código Penal de 1982**	**Código penal Español**
Articulo 214 (actual 220) Quien mediante engaño se procure o procure a un tercero un provecho ilícito en perjuicio de otro será sancionado con prisión de uno a cuatro años. La sanción se aumentará hasta un tercio cuando se cometa abusando de las relaciones personales o profesionales, o cuando se realice a través de un medio cibernético o informático.	**Articulo 190** El que mediante engaño se procure a sí o a un tercero un provecho ilícito en perjuicio de otro, será sancionado con prisión de 1 a 4 años y de 50 a 200 días-multa. La sanción será de 5 a 10 años de prisión si la lesión patrimonial excede de cien mil balboas o la cometen apoderados, gerentes administradores en ejercicio de sus funciones, o si se comete en detrimento de la administración pública o de un establecimiento de beneficencia.	**Artículo 249** 1. También se consideran reos de estafa y serán castigados con la pena de prisión de seis meses a tres años: a) Los que, con ánimo de lucro, obstaculizando o interfiriendo indebidamente en el funcionamiento de un sistema de información o introduciendo, alterando, borrando, transmitiendo o suprimiendo

	De forma supletoria **Artículo 393-A**. Quien en beneficio propio de un tercero, mediante la utilización de medios tecnológicos u otras maniobras fraudulentas, se apodere, haga uso indebido u ocasione la transferencia ilícita de los dineros, valores, bienes u otros recursos financieros de una entidad bancaria, empresa financiera u otra que capte o intermedie con recursos financieros del público o que le hayan sido confiados a ésta, será sancionado con presión de 3 a 5 años. La sanción será de 6 a 10 años de prisión, cuando el ilícito sea cometido por o con la participación de un empleado, director, dignatario, administrador o representante legal de la entidad o empresa, aprovechándose de su posición o del error ajeno.	indebidamente datos informáticos o valiéndose de cualquier otra manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro. b) Los que, utilizando de forma fraudulenta tarjetas de crédito o débito, cheques de viaje o cualquier otro instrumento de pago material o inmaterial distinto del efectivo o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero.

2.2.1. Concepto de Estafa Informática.

Según la doctrina jurídica, la estafa se encuadra dentro de la categoría de los delitos intelectivos, ya que su esencia radica en el engaño o el ardid. En este tipo de delitos, lo que prevalece es la existencia de una conducta fraudulenta que induce a la

víctima a actuar en perjuicio propio o de terceros, generando un daño económico (Arenas Nero, 2021). Es decir, se establece una clara correlación entre el acto engañoso y el perjuicio patrimonial que resulta de él. Este enfoque permite comprender la naturaleza compleja de la estafa, donde la manipulación psicológica y la astucia son elementos clave para su ejecución.

Por su parte, autores como Muñoz Conde (2015) sostiene que el denominador común de la estafa es la producción de un perjuicio patrimonial mediante una conducta engañosa, la cual induce a la víctima a caer en un error. Este autor destaca que el núcleo central de este comportamiento gira en torno a la relación causal que debe existir entre el engaño y el perjuicio. En otras palabras, no basta con que haya un engaño; es imprescindible que este engaño sea el factor determinante que provoque el daño económico. Esta perspectiva refuerza la idea de que la estafa no solo implica una acción fraudulenta, sino también una consecuencia tangible en el patrimonio de la víctima.

La estafa mediante medios tecnológicos se entiende como aquella acción con ánimo de lucro en la que un se emplea “individuo utiliza el engaño con la intención de inducir a otra persona a cometer un error, por medio de la computadora redes u otros medios. Este error lleva a la víctima a realizar un acto de disposición patrimonial que le causa un perjuicio propio o en detrimento de un tercero. Esta definición incorpora elementos esenciales para su identificación, como el engaño, el ánimo de lucro, el acto de disposición patrimonial, el error y el daño o perjuicio resultante (Tejero, 2019).

Con base a lo expuesto, la estafa informática surge como una figura necesaria para cubrir conductas defraudatorias que no encajan en la estafa tradicional, respondiendo a una dinámica delictiva derivada de los avances tecnológicos. Esta figura representa un avance en la protección del patrimonio, reformando el derecho penal clásico para enfrentar los riesgos asociados a la evolución social y tecnológica.

2.2.2. Técnicas y Tipologías de Manipulación en el Fraude.

La categoría de los delitos de estafa informática tienen sus raíces en la influencia de la doctrina alemana y española durante las décadas de los sesenta, ochenta y noventa. Esta categoría, que se refiere a la criminalidad cometida mediante el uso de tecnologías informáticas, surge a medida que la tecnología se expande en la sociedad. Como resultado, emergen modalidades delictivas que afectan nuevos intereses y causan una serie de impactos en bienes jurídicos de gran relevancia social (Mayer Lux & Oliver Calderón, 2020).

Ante este fenómeno, es relevante mencionar que la Asamblea General de las Naciones Unidas adoptó la resolución No. 65/230, que solicita a la Comisión de Prevención y Justicia Penal la creación de un grupo intergubernamental de expertos de composición abierta. Este grupo tiene como objetivo realizar un estudio exhaustivo sobre los delitos cibernéticos. A raíz de esta iniciativa, la UNODC ha llevado a cabo un análisis detallado del fenómeno de los delitos informáticos.

Es fundamental señalar lo que organismos internacionales han dicho al respecto y, de alguna manera, esclarecer el origen de la figura analizada. La ONU

(2018) clasificó los delitos informáticos en tres categorías. Una de ellas es el fraude, que se refiere a la manipulación ilegal de datos falsos o procesos dentro de sistemas informáticos con el propósito de obtener beneficios indebidos. Estos fraudes son perpetrados a través de la manipulación de computadoras y se dividen en las siguientes subcategorías:

- Fraudes derivados de la alteración de datos de entrada.
- Manipulación de programas o datos.
- Alteración de datos de salida.
- Fraude mediante la manipulación de la información.

Dentro de las categorías examinadas se encuentra la clasificación, que pueden ser como medio o como instrumento y por último se encuentra los daños a datos que consiste en generar daños por medio de virus y gusanos no autorizados por hakers o crakers.

En este mismo contexto, es relevante mencionar la alteración de datos de entrada, conocido como sustracción de datos o manipulación de entradas. Para Molina (2025) esta modalidad de ejecución se basa en la modificación de información durante la fase de adquisición. En términos simples, implica omitir la introducción de datos verídicos o insertar información falsa en un sistema informático o plataforma.

La *manipulación de datos de entrada* conlleva que el autor aporte datos incorrectos al desarrollo del programa de una computadora las cuales serán

procesados conforme a la manipulación de los datos de la computadora. Esta modalidad genérica de fraude informático conlleva la manipulación por medio de bandas magnéticas (tarjetas), discos duros, USB, o sobre un teclado.

Esto puede consistir en la creación de falsos recibos, adición de datos nuevos o la supresión de datos. En este tipo de manipulación, no afecta el funcionamiento del sistema ya que los datos suministrados funcionan ordinariamente pero con información falsa, lo que induce el error a la víctima.

Para mayor ejemplo de lo señalado, se menciona lo que se conoce como caballo de troya. Este término se refiere a la alteración del procesamiento adecuado de la información mediante modificaciones en el software o en la secuencia lógica que controla el funcionamiento del sistema informático. Esta manipulación puede ser llevada a cabo tanto por la persona que altera el programa como por aquella que introduce instrucciones en la computadora para ejecutar una función no autorizada, mientras simultáneamente realiza una tarea legítima (Garzón & Vizuete, 2009).

Es importante distinguir esta forma de manipulación de lo que se conoce como virus troyano. Este tipo de virus informático tiene como objetivo infiltrarse en el sistema haciéndose pasar por un programa aparentemente inofensivo, pero que en realidad actúa como un software que permite el control remoto del sistema afectado. Al igual que otros virus, los caballos de troya pueden modificar o eliminar archivos del sistema y tienen la capacidad de capturar información sensible, como contraseñas y números de tarjetas de crédito, para enviarla posteriormente a un destino externo.

Una de las acciones comunes asociadas a este tipo de comportamiento es la modificación de programas o datos. Esta práctica implica que el autor utiliza una consola para manipular el funcionamiento de un sistema de procesamiento de datos o de una computadora. En este contexto, se procesan datos correctos dentro del programa, que opera de manera adecuada. Sin embargo, los datos son alterados según la intención del autor. En este sentido, la salida de los datos son modificados por un ataque del hardware (Castillo González, 2016).

El siguiente comprende aquellas *manipulaciones de datos de salida*, las que se denominan output, efectuada fijando un objetivo funcional en un sistema informático, este tipo de fraude la conducta es repetida en el tiempo debido a que una vez el autor descubre o crea una laguna puede repetir la comisión del hecho punible. Uno de los ejemplos más comunes es el fraude de los cajeros automáticos mediante la falsificación de instrucciones para la adquisición de datos, actualmente se utilizan equipos informáticos sofisticados lograr estas acciones.

Para entender esta modalidad, es crucial destacar que la Corte Suprema de Justicia de Panamá, a través del Salvamento de Voto del Magistrado Jerónimo Mejía, emitió su pronunciamiento sobre un Recurso de Casación el 16 de agosto de 2022 Sentencia Penal de Corte Suprema de Justicia Panama (2022). En el núcleo de la sentencia se puede observar que el caso en cuestión es un claro ejemplo de manipulación de datos, tal como se ha mencionado anteriormente.

La conducta ilícita involucró a un empleado de una empresa, quien, con acceso autorizado como oficial de crédito, alteró información en el sistema para simular la existencia de cartas de crédito que respaldaran las operaciones de crédito con un cliente específico (una empresa). No obstante, tanto la evidencia pericial como los testimonios presentados indicaron que no existió una prueba contundente de que Mendoza tuviera la intención deliberada de engañar con ánimo de lucro ilícito o de beneficiar a un tercero de manera fraudulenta.

En este contexto, la conducta del autor del acto estuvo más vinculada a una manipulación de datos por motivos de conveniencia interna y temor a perder su empleo, que a una intención maliciosa de defraudar para obtener un beneficio económico ilícito. Este hecho puso de manifiesto la alteración de sistemas digitales y datos, y la falta de prueba concluyente sobre la intención dolosa y la existencia del engaño llevó a la Corte a concluir que no se configuró la estafa informática desde un punto de vista jurídico. La sentencia subrayó que, en ausencia de dolo, la acción no puede ser calificada como delito de estafa, sino más bien como una conducta administrativa o ética fraudulenta, y no penal.

En conclusión, la estafa informática en este caso se ejemplifica por la manipulación de datos en sistemas digitales con la finalidad de aparentar una situación que no existía, pero la ausencia de prueba de dolo suficiente llevó a la absolución del imputado. Esto resalta la importancia de demostrar claramente la intención maliciosa en delitos informáticos para que puedan calificarse como estafa y no sólo conductas irregulares o administrativas.

Otro de las modalidades en las cuales se va afincando este comportamiento, es aquellas relacionadas a *el cambio de programa*. En este caso el agente requiere sostener un conocimiento fundado sobre el discurrir del programa y sobre la programación, lo que conlleva a que el sujeto activo tenga que sostener una capacitación especial. El autor Castillo (2016) plantea una realidad que es similar con lo anteriormente señalado, ya que existe una similitud entre programa y dato.

Sin embargo, el autor apunta un aspecto relevante y es que existe una diferencia entre estos presupuestos, puesto que se incide en una diferenciación entre dato suministrado y un programa cambiado. El Programa maneja procesos en la unidad central mientras que los datos son objeto de una operación de entrada (input) y de salida (output).

Para contextualizar, es relevante destacar el caso que involucró al banco JP Morgan Chase. Este caso ilustra diversas maneras en que la manipulación y el uso indebido de sistemas informáticos han estado asociados a estafas y fraudes financieros dentro del ámbito de la estafa informática. Por lo tanto, este incidente sirve como un claro para comprender el concepto de manipulación de programas, siendo significativo en el sector bancario, donde la gran capacidad informática y los sistemas complejos permiten que modificaciones malintencionadas puedan causar graves daños al patrimonio de terceros.

Un caso relevante que ilustra la manipulación de programas es el de Hernán Arbizu, quien se desempeñó como ex vicepresidente del JP Morgan Bank. Durante su tiempo en el banco, Arbizu logró manejar de manera clandestina varias cuentas y realizar transferencias no autorizadas, evidenciando el uso indebido de los sistemas internos de la entidad para llevar a cabo operaciones ilícitas.

Esta situación se vio facilitada por la manipulación de los sistemas y la falta de controles adecuados, así como por una gestión deficiente, lo que permitió que un empleado tuviera acceso y pudiera alterar datos y fondos sin autorización. Esto resalta la importancia del manejo seguro de los sistemas informáticos internos (Juzgado Criminal y Correccional Federal Nro. 12, 2008).

Las acciones ilícitas que se pueden identificar en esta situación están relacionadas con la omisión de reportar las transacciones efectuadas, producto de la manipulación de los sistemas de monitoreo y la evasión de los análisis de riesgo del lavado de dinero. Además, se evidencia una ausencia de algoritmos efectivos que permitan detectar transacciones o patrones sospechosos.

El caso permite extraer un concepto claro de la aparición de esta modalidad, ya que los programas son tratados dentro de una unidad de procesamiento de datos, por tanto, la diferencia que existente entre manipulación de datos o programas se centra en el contenido de los datos almacenados y sus diferentes funciones. Es por ello que según el autor Castillo González (2016,p.78) destaca lo siguiente:

El objeto y el medio de la manipulación de entrada y la manipulación de

programas no se diferencia significativamente si el programa desde el inicio se cambiaron los datos, porque se aportan nuevos datos o porque se borraron datos existentes. Caso igual en los casos de cambio de programa, aspecto que solo es posible por los aportes a los datos de entrada que cambian las ordenes de los programas".

El último aspecto relevante se refiere a la *manipulación de datos de salida*. Este término hace referencia a los resultados generados por un sistema de procesamiento de datos. En este contexto, el autor altera o falsifica los resultados correctos producidos por la computadora, logrando que se imprima un resultado diferente al que realmente corresponde (Estrada & Ramos, 2011). En este contexto, es importante señalar que la manipulación de datos puede llevarse a cabo sin la intervención directa de una computadora, ya que implica la falsificación del adecuado sistema de procesamiento de información.

La jurisprudencia panameña ofrece un claro ejemplo de esta problemática a través de la sentencia de Casación emitida el 21 de febrero de 2017, con el Magistrado José Ayu Prado Canals como ponente. Al examinar los hechos subyacentes a esta decisión, se evidencia una situación en la que se establece una relación ilícita entre la manipulación de datos y accesos no autorizados a sistemas informáticos. Esto se sitúa dentro de un marco de estafa electrónica, que incluye intentos de interferencia y la apropiación ilegal de información digital (Ayu Prado, 2017).

En el fallo mencionado, se observa que un grupo de individuos accedió de manera no autorizada al sistema de una empresa privada y a sus clientes, utilizando credenciales válidas y vulnerando las medidas de seguridad existentes. Esta acción fue factible debido a que los atacantes poseían información sobre la plataforma, incluidas contraseñas y configuraciones internas. Se concluye que los intrusos obtuvieron acceso mediante credenciales de administración, lo que sugiere que las claves tenían conocimiento previo o fueron obtenidas de manera ilícita, lo que permitió la manipulación de los sistemas internos.

En cuanto al contexto de los hechos, se pudo determinar que los ataques provienen de direcciones IP que pertenecen a redes internas de la empresa, específicamente desde Cable Onda y Telefónica de Argentina, lo que indica que los atacantes lograron alterar rutas y registros de acceso, modificando los logs para encubrir su origen real.

Este caso, es un claro ejemplo de cómo las actividades ilícitas se manifestaron en accesos no autorizados a sistemas internos mediante técnicas de hacking, capitalizando sobre credenciales y vulnerabilidades en las configuraciones de seguridad. Esto permitió la manipulación de datos y, a su vez, la eliminación y alteración de información crítica de las empresas afectadas. La manipulación de programas y registros internos fue una estrategia clave para ocultar las acciones de los responsables, dificultando su identificación y causando un daño considerable a los sistemas, datos y operaciones de las víctimas.

En el caso analizado, se ha observado que los datos y programas fueron alterados de tal forma que se volvió imposible rastrear la fuga de información valiosa perteneciente a la empresa afectada, la cual incluía cuentas, documentos y otros datos cruciales. Un aspecto importante a resaltar es que los perpetradores cuentan con habilidades especializadas y un amplio conocimiento del entorno, lo que les permite identificar las alternativas más ventajosas. Esto les facilita seleccionar el momento propicio para llevar a cabo sus engaños en los sistemas informáticos, con el fin de minimizar la trazabilidad de sus acciones.

Es fundamental que el lector se enfoque en que la manipulación de los datos de salida, se traduce en la falsificación de información correctamente generada por el sistema de procesamiento de datos, o en la obstrucción de la impresión de los mismos. La doctrina contemporánea ha avanzado en la clasificación de delitos, centrándose en aquellos que atentan contra el patrimonio económico de las personas. Diversos autores y organismos han propuesto distintas categorizaciones de la estafa, que se entrelazan con las modalidades de manipulación previamente identificadas.

En este sentido, las formas de manipulación representan las *técnicas delictivas utilizadas* para manejar datos de manera fraudulenta, mientras que los tipos de estafa son las incidencias comunes asociadas a estas modalidades. Entre las variantes más reconocidas de la estafa conforme a la doctrina y legislaciones internacionales, se destacan las siguientes:

- Pharming

- Phishing
- Smishing
- Vishing
- Carding

Así como la falsa venta o alquiler fraudulento de bienes y la estafa nigeriana. Todas ellas son reflejo de un trabajo de ingeniería social, donde el objetivo del fraude es clave para la ejecución del hecho punible. Ante este escenario la doctrina ha ubicado una serie de comportamientos tipológicos que se han desarrollado a través de la literatura de este tema de los cuales se resalta los siguientes:

2.2.2.1. El Pharming

El pharming es una técnica de manipulación de la resolución de nombres en internet que lleva a cabo un código malicioso comúnmente en forma de troyano, que se instala en un ordenador durante el proceso de descargas, a través de correos electrónicos no deseados (spam), mediante copias desde CD-ROMs, entre otros métodos.

La palabra pharming deriva del término farm (granja) y está relacionada con el término phishing, utilizado para nombrar la técnica de ingeniería social que, mediante suplantación de correos electrónicos o páginas web, intenta obtener información confidencial de los usuarios, desde números de tarjetas de crédito hasta contraseñas. La etimología de esta palabra se halla en que una vez que el atacante ha conseguido acceso a un servidor DNS y tomado control de éste, es como si

poseyera una granja donde puede hacer uso a placer de los recursos que allí se encuentran (Rodríguez, 2009).

El pharming implica que, al tener nuestro ordenador infectado por un troyano o un programa que altera las configuraciones de las DNS, este intenta acceder a un sitio web mediante la URL de una página falsa, donde la persona confía que es la legítima. Como resultado, la persona podría realizar compras o acceder a cuentas bancarias sin darse cuenta de que está entregando sus datos confidenciales a los delincuentes, quienes a su vez podrían utilizar información del cliente para llevar a cabo fraudes (Callegari, 2022).

Ahora bien, es importante indicar que el pharming y el phishing son tipos de ciberataques que a menudo se confunden, pero tienen enfoques distintos. Mientras que el phishing utiliza técnicas de ingeniería social para engañar a los usuarios a que revelen información personal mediante correos electrónicos o sitios web falsos, el pharming redirige a los usuarios a sitios fraudulentos sin requerir interacción directa.

En un ataque de phishing, un usuario recibe un correo electrónico que aparenta ser de su banco, instándole a hacer clic en un enlace para ingresar sus credenciales. En cambio, el pharming opera de manera más insidiosa: un usuario puede escribir correctamente la URL de su banco y, aun así, ser redirigido a un sitio falso que imita al original. Esta técnica hace que el pharming sea más difícil de detectar, ya que las víctimas a menudo no son conscientes de que han sido comprometidas.

Para ejemplificar esta forma de estafa digital, consideremos un ciberataque que impactó a la República de Brasil el 30 de junio de 2025. Este incidente se clasifica como uno de los ciberataques más significativos en la historia del sistema financiero brasileño, lo que comprometió gravemente la confianza en los pagos instantáneos a través de PIX. A su vez, destacó las vulnerabilidades presentes en los sistemas críticos y en la cadena de suministro dentro del sector financiero (Martínez, 2025).

Los hechos que sustentan este caso es un empleado de C&M Software, este fue víctima de un ataque de ingeniería social. Mediante esta táctica, los atacantes lograron obtener acceso no autorizado a las credenciales internas, incluyendo claves privadas y certificados digitales críticos para la firma de transacciones. Con estos recursos, los delincuentes llevaron a cabo miles de transacciones fraudulentas, desviando fondos cuya estimación varía entre 80 y 800 millones de dólares, que posteriormente fragmentaron en criptomonedas para dificultar su rastreo.

La operación se extendió durante varios días, afectando a diversas instituciones que dependían de C&M, generando un efecto en cadena que paralizó el procesamiento de transacciones y, en consecuencia, debilitó la confianza en el sistema de pagos instantáneos PIX y en el ecosistema financiero en general. Este caso pone en evidencia cómo las vulnerabilidades humanas y la gestión inadecuada de credenciales pueden ser explotadas en ataques sofisticados con consecuencias sistémicas de gran escala.

Este incidente se distinguió por la manipulación de credenciales, el acceso a infraestructuras críticas y la ejecución de movimientos financieros fraudulentos. Estos elementos presentan ciertos aspectos fundamentales en común con una estafa informática que utiliza la técnica de pharming.

En el contexto de Brasil, los delincuentes no llevaron a cabo una redirección típica de sitios web; en cambio, lograron realizar transacciones fraudulentas dentro del sistema de pagos instantáneos (PIX) mediante la obtención y uso indebido de credenciales internas y certificados digitales. A pesar de las diferencias en la técnica empleada, ambos enfoques persiguen el mismo objetivo: engañar y manipular a usuarios o sistemas para redirigir transacciones o información hacia destinos controlados por los atacantes.

En este caso, un empleado fue víctima de ingeniería social, lo que le llevó a entregar sus credenciales, un procedimiento común en diversos ataques de pharming, donde se engaña a los usuarios para que crean que están en sitios auténticos. En resumen, el ataque en Brasil puede considerarse una forma avanzada de estafa informática que comparte principios con pharming, ya que ambos, aunque a través de distintas técnicas, manipulan sistemas y la confianza de los usuarios para desviar recursos y robar información o dinero. La principal diferencia radica en el nivel y la forma de ejecución, siendo uno la redirección de la web y el otro la manipulación de certificados y credenciales en sistemas internos.

2.2.2.2. Phishing

Proviene del inglés fishing (pesca) y hace referencia a la idea de que los usuarios caen en la trampa, similar a los peces que muerden el anzuelo. La primera vez que se utilizó esta expresión fue en 1996, en el boletín de noticias Hacker 2600 Magazine.

Es importante señalar que el phishing es una técnica que combina la ingeniería social con vulnerabilidades técnicas, con el objetivo de engañar a la víctima para que revele información personal. Esta táctica se emplea principalmente para obtener beneficios económicos por parte del atacante. Generalmente, los ataques de phishing comienzan con el envío de correos electrónicos fraudulentos que contienen un enlace (URL) engañoso (Valle Matute, 2013).

En otras palabras, el escenario del phishing generalmente está asociada con la capacidad de duplicar una página web para hacer creer al visitante que se encuentra en el sitio web original en lugar del falso. Este tipo de engaño suele llevarse a cabo a través correo electrónico y a su vez estos correos contiene enlaces a un sitio web falso con una apariencia casi real a sitio legitimo.

Al hacer clic en este enlace, la víctima es redirigida a un sitio web fraudulento. A pesar de la amplia atención que este problema ha recibido durante los años, aún no se ha implementado una solución definitiva para contrarrestar este tipo de ataque. En términos simples, una página de phishing es aquella que, sin permiso, se presenta como si fuera un representante de una entidad legítima, con el fin de engañar a los usuarios para que realicen acciones específicas.

Esta problemática se ha exacerbado con el envío de correos SPAM, que invitan a las personas a acceder a una página falsa con el objetivo de robar información confidencial, como contraseñas, números de tarjetas de crédito o datos financieros. Frecuentemente, estos correos llegan a la bandeja de entrada y se disfrazan de comunicaciones provenientes de departamentos de recursos humanos, tecnología o áreas comerciales relacionadas con transacciones financieras.

Para respaldar esta afirmación, la prensa de Panamá publicó una serie de alertas emitidas por el Banco General en las cuales se detalla que sus sitios web, han sido objeto de intentos de fraude a través de esquemas de phishing, lo que ha generado confusión entre sus clientes. El Banco enfatizó que nunca solicita actualizaciones de información a través de enlaces en correos electrónicos. Además, explicó que en estos fraudes, los delincuentes envían mensajes falsos que pretenden imitar a sitios web auténticos, logrando así engañar a muchas personas que los perciben como oficiales y confiables (La Prensa, 2009).

La modalidad delictiva en cuestión se lleva a cabo a través de faxes y mensajes SMS dirigidos a un público amplio, promoviendo premios y descuentos en productos. Estos mensajes se envían de manera masiva, con el objetivo de que un pequeño porcentaje de usuarios caiga en la trampa. Según una publicación del periódico el capital financiero (2024) en Panamá se ha registrado un aumento del 24% en estafas por mensajes falsos. A nivel regional, los fraudes que utilizan inteligencia artificial, como audios y videos deepfake están en auge, convirtiéndose

en una de las principales tendencias delictivas. Estos métodos facilitan engaños más convincentes, especialmente en redes sociales.

Entre julio de 2023 y julio de 2024, América Latina experimentó aproximadamente 397 millones de bloqueos de phishing y más de 697 millones de intentos de fraude. Brasil, México y Perú se destacan como los países más afectados. Los ciberdelincuentes han comenzado a utilizar herramientas de inteligencia artificial, incluso dominios de IA para crear sitios web falsos que engañan a las víctimas, provocando un aumento exponencial en las estafas digitales. Los expertos predicen que estas técnicas son de bajo costo y alta escalabilidad que seguirán creciendo en los próximos años, impulsadas por la creatividad de los criminales y el acceso a tecnologías avanzadas.

En conclusión, el phishing representa una amenaza significativa en la ciberseguridad, caracterizada por el uso de la ingeniería social y vulnerabilidades técnicas para engañar a las víctimas y obtener beneficios ilícitos. Esta modalidad delictiva ha evolucionado con el tiempo, adoptando formas cada vez más sofisticadas, como la inteligencia artificial, los deepfakes y la creación de sitios web falsos con dominios específicos, lo que ha aumentado su efectividad y alcance.

A pesar de las campañas de concientización y los esfuerzos por combatir este fenómeno, no se ha encontrado una solución definitiva que erradique completamente el phishing, que sigue generando millones de intentos de fraude a nivel global. En el contexto panameño, la creciente incidencia de estafas a través de mensajes falsos

subraya la urgente necesidad de fortalecer los sistemas de alerta y protección, tanto a nivel institucional como individual.

La continua innovación de los ciberdelincuentes impulsada por el acceso a tecnologías asequibles, indica que el phishing seguirá siendo una problemática relevante y en constante aumento. Por lo tanto, es crucial implementar medidas preventivas eficaces y promover una cultura de seguridad digital entre los usuarios para mitigar esta amenaza.

Siguiendo esta misma línea se tiene otra modalidad dentro del phishing denominada *Smishing* que se manifiesta a través del envío de mensajes de texto a teléfonos móviles, los cuales a menudo ocultan el número de teléfono del remitente, presentando en el mensaje direcciones web, enlaces o links que se asemejan a páginas institucionales de empresas o entidades públicas.

La vulnerabilidad se produce cuando el usuario clickea en el link, lo que puede llevarlo a una página de phishing o en algunos casos, a infectar su dispositivo con un código malicioso y en ese mismo sentido se tiene el Vishing que se refiere a prácticas delictivas donde el delincuente envía mensajes de texto haciéndose pasar por una institución bancaria, solicitando que el usuario se comunique con un número falso o le pide que responda al SMS revelando información confidencial, como números de tarjeta o claves (Colina Moreno & Larios Rodríquez, 2024).

Otro de las modalidades, que es muy permanente en Panamá es el *Carding*, que resulta en una acción delictiva que implica la copia de tarjeta de crédito o débito de una persona, permitiendo a los delincuentes acceder a los fondos disponibles de la víctima para adquirir bienes. Algunos expertos consideran que esta práctica se encuentra dentro de la categoría de estafa en línea, ya que las compras realizadas suelen ser de montos pequeños y se acumulan a lo largo del tiempo, perjudicando así al titular de la cuenta.

La República de Panamá enfrenta un alarmante aumento de casos de clonación de tarjetas de crédito. Un fallo de la Corte Suprema de Justicia, emitido en marzo de 2021, confirmó la detención preventiva de un acusado tras una investigación que reveló la operación de un individuo en un edificio de Panamá. Durante los allanamientos, se descubrieron múltiples equipos electrónicos, chips de varias compañías telefónicas, dispositivos de clonación y otros elementos asociados a actividades fraudulentas y delictivas contra el patrimonio económico.

Las denuncias y testimonios de empresas afectadas establecen un sólido vínculo entre el imputado y delitos que amenazan la estabilidad del sistema de telecomunicaciones, generando significativas pérdidas económicas. Aunque estos delitos se asemejan al carding, se inscriben en un contexto diferente, como el tráfico ilegal de llamadas y la clonación de chips. La decisión judicial reafirma que el proceso se ajusta a los requisitos legales y que la conexión del acusado con estos delitos es suficiente para justificar la orden de prisión preventiva, subrayando la

relevancia de la evidencia tecnológica en la lucha contra los delitos informáticos y patrimoniales.

El análisis del fallo judicial en relación con el delito de carding revela aspectos clave sobre la naturaleza y percepción jurídica de los fraudes y el uso ilícito de tecnologías informáticas. En este caso, la Corte Suprema de Justicia de Panamá ratificó la legalidad de la detención preventiva del sujeto, vinculado a delitos patrimoniales económicos. Su participación implicó el uso de equipos electrónicos y software para la clonación de chips telefónicos, el tráfico de llamadas ilegales y otros fraudes mediante la manipulación de sistemas de comunicación.

La investigación halló equipos tecnológicos sofisticados, como gateways VOIP, tarjetas SIM y teléfonos celulares, utilizados para realizar llamadas internacionales de manera ilícita, lo que perjudica tanto a las empresas de telecomunicaciones como al Estado. Este caso es análogo al fenómeno del carding, donde se utilizan tecnologías avanzadas para realizar fraudes financieros, comprometiendo la seguridad de los sistemas y erosionando la confianza en las operaciones digitales.

No obstante, mientras el carding se enfoca en el robo de datos de tarjetas de crédito y débito, el fallo judicial aborda actividades ilícitas relacionadas con el tráfico de llamadas y la clonación de chips, generando pérdidas económicas significativas. Ambos delitos comparten la explotación de vulnerabilidades tecnológicas y la capacidad de los delincuentes para manipular sistemas, pero difieren en sus

objetivos: el carding busca fraudes financieros directos, mientras que el caso analizado se centra en la evasión de controles en telecomunicaciones.

La decisión judicial también subraya la relevancia de la investigación y la evidencia tecnológica como fundamentos esenciales en la lucha contra los delitos informáticos y sus diversas manifestaciones en la actualidad. Otras de las modalidades de estafa informática se resalta la estafa nigeriana, siendo esta una técnica fraudulenta en la que el autor se pone en contacto con la víctima a través de correos electrónicos, mensajes o redes sociales, prometiendo una considerable suma de dinero a cambio de un pago inicial. Esta práctica se asemeja a los tradicionales timos como el tocomocho o el timo de la estampita, pero ha evolucionado en el entorno digital.

Esta modalidad de estafa aprovecha los canales electrónicos, y se conoce popularmente como cartas nigerianas debido a que en sus inicios, muchos de los perpetradores eran ciudadanos de Nigeria o de otras naciones africanas. Este tipo de engaño genera en la persona un falso sentido de oportunidad para obtener dinero mediante gestiones que parecen sencillas.

Este es el gancho utilizado por los ciberdelincuentes para que las posibles víctimas ignoren las precauciones más básicas y terminen siendo defraudadas. Generalmente, el remitente se presenta como un abogado, un amigo, un familiar o un funcionario gubernamental, buscando establecer una conexión que sitúe a la persona

en una posición de vulnerabilidad, facilitando así la realización de la transacción fraudulenta.

Para subrayar la importancia de este comportamiento en la actualidad, es necesario destacar lo que ha informado la agencia internacional INTERPOL sobre uno de los casos de estafas nigerianas más significativos en tiempos recientes. Este caso involucra a un ciudadano nigeriano de 40 años conocido como Mike, quien fue el perpetrador de fraudes que sumaron un total de 60 millones de dólares, afectando a cientos de víctimas alrededor del mundo.

En uno de los casos, una víctima perdió la asombrosa suma de 15,4 millones de dólares. El modus operandi de este individuo se basaba en el uso de correos electrónicos de pequeñas y medianas empresas en varios países, incluyendo Australia, Canadá, India, Malasia, Rumania, Sudáfrica, Tailandia y Estados Unidos. Las principales víctimas de estas estafas eran otras empresas que habían caído en la trampa de las cuentas comprometidas.

El líder de la red de cibercrimen en Nigeria, Malasia y Sudáfrica, fue arrestado en Port Harcourt, Nigeria, tras una investigación colaborativa entre INTERPOL y la Comisión de Delitos Económicos y Financiaros (EFCC). Este individuo, que operaba con al menos 40 cómplices, se especializaba en fraudes cibernéticos, incluyendo el fraude de desvío de pagos y el fraude del CEO. El modus operandi incluía comprometer las cuentas de correo electrónico de proveedores y ejecutivos para desviar pagos a cuentas bajo su control. Las autoridades pudieron rastrear a este

individuo gracias a un informe de Trend Micro y un análisis realizado por Fortinet Fortiguard Labs, lo que permitió a los expertos de INTERPOL y la EFCC localizarlo y proceder con su arresto en junio.

El jefe Delitos Cibernéticos de la EFCC, destacó la complejidad de los fraudes asociados al correo electrónico empresarial y enfatizó que Nigeria no debe ser considerada un refugio seguro para los ciberdelincuentes. En la cooperación entre el sector público y privado, se subraya la importancia de esta colaboración para desmantelar organizaciones criminales transnacionales. El sospechoso junto a otro cómplice de 38 años enfrenta múltiples cargos, incluidos piratería informática e conspiración, actualmente se encuentran en libertad bajo fianza mientras continúa la investigación (INTERPOL, 2016).

Estos casos recientes evidencian que las distintas modalidades de ciberataques, como el pharming, el phishing, el smishing, el vishing, el carding y las estafas nigerianas, comparten un objetivo común: manipular sistemas y la confianza de los usuarios para obtener beneficios ilícitos. Aunque cada técnica presenta particularidades en su ejecución, todas aprovechan vulnerabilidades tanto técnicas como humanas, demostrando la creciente sofisticación de los delincuentes en el entorno digital.

La evolución constante de estas amenazas, impulsada por el acceso a nuevas tecnologías y herramientas como la inteligencia artificial, subraya la urgente necesidad de fortalecer las medidas de protección, concienciar a los usuarios y

promover una cultura de seguridad digital. La persistencia y adaptación de estos delitos demandan respuestas integradas y actualizadas para mitigar su impacto en la seguridad y estabilidad de los sistemas financieros y de comunicación, especialmente en contextos vulnerables como el de Panamá y América Latina.

A continuación, se presentará un cuadro que ofrece una visión comparativa de diversas formas de delitos cibernéticos, los cuales fueron ampliamente detallados en líneas anteriores. Cada uno de estos conceptos se define en términos de su mecanismo, similitud y diferencias claves, permitiendo al lector comprender sus características principales y particularidades que los distinguen del panorama de la ciberdelincuencia. Esta comparación es fundamental para contextualizar las amenazas digitales actuales y potenciar las estratégicas de protección y prevención frente a estos delitos.

Tabla 2. Comparación de los diferentes tipos de delitos informáticos

Concepto	Definición	Similitudes	Diferencias
Pharming	Manipulación de DNS mediante malware (ej. troyanos) para redirigir a páginas falsas.	- Busca robar datos confidenciales. - Utiliza ingeniería social y técnicas técnicas.	- Enfoque técnico (DNS). - No requiere interacción directa del usuario (solo acceder a URL).
Phishing	Correos electrónicos fraudulentos con enlaces a sitios falsos para obtener información.	- Engaña mediante suplantación de identidad. - Fines económicos.	- Canal principal: correo electrónico. - Requiere acción del usuario (hacer clic).
Smishing	Mensajes de texto (SMS) con enlaces maliciosos que	- Suplantación de identidad.	- Canal: SMS. - Puede infectar dispositivos con

	simulan ser instituciones legítimas.	- Vinculado a phishing.	malware al hacer clic.
Vishing	Llamadas o mensajes de texto falsos (suplantando bancos) para obtener datos directamente.	- Objetivo: información confidencial. - Relacionado con phishing.	- Canal: voz (llamadas) o SMS. - Interacción directa (ej. pedir claves por teléfono).
Carding	Robo de datos de tarjetas (clonación, phishing) para compras fraudulentas.	- Finalidad económica. - Usa técnicas como phishing.	- Enfoque en datos de tarjetas. - Transacciones pequeñas para evadir detección.
Falsa venta	Simulación de venta/alquiler de bienes para recibir pagos sin entregar el producto.	- Engaño para obtener dinero. - Uso de medios digitales.	- No requiere robo de datos. - Víctima paga voluntariamente por un servicio/producto falso.
Estafa Nigeriana	Ofrecimiento de grandes sumas de dinero a cambio de un pago inicial (ej. herencias).	- Engaño mediante promesas irreales. - Adaptación digital de estafas clásicas.	- No implica suplantación de identidad. - Se basa en la codicia de la víctima.

En el cuadro anterior, se confirma que todas estas modalidades delictivas persiguen como objetivo final obtener beneficios económicos mediante el engaño. No obstante, los métodos y los canales empleados varían. En el análisis de las técnicas utilizadas en la ciberdelincuencia es fundamental clasificarlas según su complejidad técnica y su relación con la ingeniería social. Esta clasificación permite comprender mejor el funcionamiento de los ataques y las medidas de prevención.

A continuación, se dividirá dichas técnicas en dos grupos, las de enfoque técnico como el pharming y el carding, que dependen de herramientas tecnológicas y las que se sustentan principalmente en la manipulación psicológica, como la estafa nigeriana. Otro criterio es la interacción en el pharming que opera de forma silenciosa, mientras que el vishing y la venta falsa exigen un diálogo directo. Por último, está el aspecto de la monetización, algunas técnicas (pharming, carding) actúan como intermediarias y roban datos para venderlos, mientras que otras (venta falsa) buscan obtener ganancias inmediatas.

Tabla 3. Similitudes y diferencias de los tipos de delitos informáticos.

Concepto	**Definición**	**Similitudes**	**Diferencias**
Pharming	Manipulación de DNS mediante malware (ej. troyanos) para redirigir a páginas falsas.	- Busca robar datos confidenciales. - Utiliza ingeniería social y técnicas.	- Enfoque técnico (DNS). - No requiere interacción directa del usuario (solo acceder a URL).
Phishing	Correos electrónicos fraudulentos con enlaces a sitios falsos para obtener información.	- Engaña mediante suplantación de identidad. - Fines económicos.	- Canal principal: correo electrónico. - Requiere acción del usuario (hacer clic).
Smishing	Mensajes de texto (SMS) con enlaces maliciosos que simulan ser instituciones legítimas.	- Suplantación de identidad. - Vinculado a phishing.	- Canal: SMS. - Puede infectar dispositivos con malware al hacer clic.
Vishing	Llamadas o mensajes de texto falsos (suplantando	- Objetivo: información confidencial.	- Canal: voz (llamadas) o SMS. - Interacción directa (ej. pedir

	bancos) para obtener datos directamente.	- Relacionado con phishing.	claves por teléfono).

Tabla 4. Diferencia por criterio

Criterio	Pharming	Carding	Phishing/Smishing	Vishing	Falsa venta	Estafa Nigeriana
Técnicas vs. Social	Técnico (malware, redirección DNS)	Técnico (clonación de tarjetas)	Combinación (ingeniería social + enlaces/archivos)	Combinación (ingeniería social + llamadas)	Puramente social	Puramente social
Interacción con víctima	Pasiva (redirección automática)	Variable (depende de uso de datos robados)	Requiere acción (clic en enlace/archivo)	Exige comunicación directa (llamada/respuesta)	Interacción activa (negociación falsa)	Interacción prolongada (manipulación emocional)
Objetivo principal	Robar datos (ej. credenciales)	Robar datos financieros (ej. información de tarjetas)	Robar datos (credenciales, información personal)	Robar datos (ej. códigos OTP, datos bancarios)	Obtener dinero directo (pagos por productos/servicios falsos)	Obtener dinero directo (avances de fondos con promesas falsas)

CAPÍTULO III. Análisis dogmático del delito de Estafa por medios informáticos en Panamá.

3.1. CUESTIONES FUNDAMENTALES

3.1.1. Introducción al Delito de Estafa Informática.

La estafa se define como una forma de defraudación que no solo afecta la propiedad en sí, sino que impacta en la integridad del patrimonio. En términos generales, la estafa puede entenderse como el acto que una persona causa de un error inducido por la conducta del agente, realiza una disposición patrimonial

desfavorable que el agente busca en convertir en un beneficio propio o de un tercero (Echavarría Ramírez, 2022).

En términos generales la cadena causal de la estafa, al igual que cualquier defraudación, se desarrolla de la siguiente manera, el agente lleva a cabo una actividad engañosa que genera un error en la víctima. Como consecuencia de este error la victima efectúa una acción que resulta perjudicial para su patrimonio. Por tanto la conducta punible radica en defraudar a través de engaños o artimañas (López et al., 2024).

En Panamá, el castigo para la estafa está contemplada en el artículo 220 del Código Penal. Esta norma establece una serie de requisitos normativos que son fundamentales tanto para la tipicidad objetiva como subjetiva, los cuales son esenciales para demostrar la existencia del tipo penal. Un componente fundamental de la estafa en medios informáticos es el engaño, que actúa como el elemento central de este tipo de fraudes. De manera más precisa, se refiere a lo establecido en un fallo de la Corte Suprema de Justicia, el cual textualmente expresa lo siguiente:

“El engaño consiste en un proceso intelectual de convencimiento en el cual una persona crea una convicción en otra para inducirla a error y así obtener un lucro indebido de ella” (Guerra De Villalaz, 2002, p.112). Lo anterior denota que la estafa lleva consigo la disposición del sujeto pasivo de entregar un bien mueble o inmueble; sin embargo, dicha voluntad se encuentra viciada por el engaño y artificio del sujeto

activo, quien no cumplirá con lo acordado (Sentencia Civil de Corte Suprema de Justicia Panama, 1ª de lo Civil, 2014).

Partiendo de lo anterior, se tiene que el engaño va de manera entrelazada con los fines propuestos por el sujeto activo de cuál sea su modalidad, debiendo tener adecuada entidad para generar un estímulo de traspaso. Por lo tanto, se entiende que el engaño debe ser eficaz con la intención de que el sujeto caiga en el error, siendo el error otro aspecto importante a destacar en el contexto de una estafa, ya que debe ser de carácter esencial sobre la víctima.

Esto implica que bajo su influencia, la persona actúa sin sospechar que sus decisiones tendrán repercusiones negativas en su patrimonio (Rodríguez de Oliveira, 2025). Este punto nos conduce a analizar nuestra tercera hipótesis: el acto de disposición patrimonial. Este término se refiere a la acción realizada por la persona afectada que beneficia al estafador pero perjudica a la víctima.

Ante lo expuesto, se señala que todo acto que implique un desplazamiento patrimonial en perjuicio de la víctima se incluiría en esta categoría, ya sea a través de una entrega tangible o simplemente como un movimiento contable. También podría tratarse de algún servicio que sea susceptible de cuantificación económica.

Esta reflexión lleva a identificar tres elementos fundamentales que constituyen los requisitos de la estafa, los cuales son el perjuicio, el ánimo de lucro y el nexo causal. Abordar estos componentes permitirá entender más a fondo la naturaleza del

delito y sus implicaciones legales. Para ilustrar este razonamiento, se hace énfasis a la Corte Suprema de Justicia, firmada por el magistrado ponente Harry Díaz, el 29 de agosto de 2014, donde se establece que, para que se consuma la lesión, el sujeto activo debe tener la intención de causar un perjuicio efectivo, y no simplemente una amenaza sobre el patrimonio del afectado (Sentencia Pleno de Corte Suprema de Justicia (Panama, Pleno, 2 de Julio, 2014).

Por tanto, al analizar el verbo *obtener* en el contexto de la conducta ilícita, es crucial destacar que implica una intención clara de enriquecimiento a expensas de otro. Este enriquecimiento se manifiesta a través de la realización de actos que, aunque pueden parecer legítimos en la superficie, en última instancia buscan menoscabar el patrimonio ajeno.

En este sentido, la conducta delictiva no solo se circunscribe a la mera intención de causar un daño, sino que se establece como un proceso deliberado donde el actor planifica y ejecuta acciones con el objetivo de adquirir un beneficio económico. Así, la noción de provecho ilícito se convierte en un elemento fundamental, ya que revela la naturaleza de la acción como contraria a la ley y a las normas de convivencia establecidas.

Es decir, la efectividad de la consecución de este beneficio debe ser medible y palpable, lo que implica que no basta con la intención de perjudicar al prójimo; es esencial que se materialice un daño patrimonial que claramente afecte a la víctima. Esta dinámica resalta la relación entre el verbo obtener y los conceptos de

imputación y responsabilidad penal, en tanto que la ley asegura que quien actúa con voluntad de lucro a costa del patrimonio de otro debe enfrentar las consecuencias de sus actos.

Por otro lado, es importante considerar que el perjuicio patrimonial sufrido por la víctima puede adoptar diversas formas y manifestarse a través del despojo físico de bienes, daños a la propiedad o mediante fraudes económicos que, aunque no impliquen un despojo físico, generan una pérdida significativa en el valor de los activos de la víctima. Esta diversidad en la manifestación del daño resalta la amplitud de la interpretación del verbo obtener que comprende todas las modalidades en que se puede infligir perjuicio al patrimonio ajeno por parte del agente. En este sentido, no se exige que el aprovechamiento obtenido se agote o se perfeccione.

El perjuicio reportado por la víctima debe ser siempre patrimonial, de modo que su patrimonio debe verse disminuido de forma efectiva y objetiva, sin que medie contraprestación alguna para el sujeto activo. De acuerdo con esto, en el delito de estafa, el agente debe inducir a error o mantener al sujeto pasivo en el error mediante artificios o engaños. Estos son los medios destinados a confundir al sujeto pasivo, convenciendo a este de una falsedad. Por lo tanto, el inductor se convierte en la causa mediata y real del juicio equivocado o de la idea falsa (Gonzáles, 2014).

El último elemento a explicar es el nexo causal, el cual se encuentra ligado a la teoría de la imputación objetiva ligada a la relación tripartita entre engaño, error y disipación patrimonial (Roxin et al., 2003). Esto responde a que la estafa se basa en

la simulación y la astucia como una forma ambigua en el que el sujeto activo comienza con un engaño que induce a un error a la víctima.

En el párrafo anterior, se expusieron los elementos fundamentales de la estafa dentro del marco objetivo del tipo penal. Sin embargo, el enfoque principal de esta investigación es identificar aspectos que podrían contribuir a una legislación penal más efectiva. Para ello, es crucial analizar los momentos en las que no se encuentran todos los elementos del tipo penal, especialmente en el contexto de la estafa informática.

Esto, lleva a examinar la tipicidad en el delito de estafa informática, donde no siempre existen un sujeto que engaña y otro que es engañado (Calle Rodríguez, 2007). En este ámbito, se observan conductas penales que no encuadran adecuadamente en la definición tradicional del delito, ya que frecuentemente falta alguno de sus elementos esenciales, como el sujeto engañado.

Por ejemplo, con respecto al *spyware y phishing*, la relación típica de engaño se ve comprometida. En el caso del spyware, un programa malicioso se instala en el ordenador de la víctima sin que esta sospeche, lo que lleva a un perjuicio ulterior sin la interacción activa de un engañador. En el phishing, aunque hay un engaño inicial para que la víctima entregue sus claves personales, una vez que se obtienen los datos sensibles, no es necesario más contacto entre los involucrados.

De este modo, en este último caso tampoco se da un engaño ni error que motive una variación en el patrimonio de la víctima. Esta reflexión subraya la complejidad del delito de estafa informática, indicando la necesidad de una revisión legislativa que contemple estas particularidades. Es fundamental abordar de manera específica los delitos relacionados con la estafa informática, con el objetivo de incluir situaciones que anteriormente no eran claras ni podían encuadrarse dentro de los tipos penales existentes.

La estafa informática se caracteriza por que la transmisión patrimonial no es realizada por la víctima bajo engaño, sino que es el propio autor quien a utilizado artificios tecnológicos y medios informáticos que lleva a cabo el acto delictivo. En muchas ocasiones, esta acción se produce sin que exista una fase previa de engaño, a diferencia de lo que ocurre en la estafa convencional.

3.2. El tipo penal de la Estafa. cambiar índice

El comportamiento habitual expuesto en el artículo 220 define una modalidad delictiva cuya finalidad es la defraudación de carácter patrimonial. Esta modalidad se compone de acciones que buscan simular hechos falsos, dirigidos a un individuo que se intenta engañar.

Las consideraciones sobre el tipo penal de la estafa, nos llevan a explicar a continuación acerca de las características de éste, como son delito de resultado de lesión, de ejecución instantánea y de carácter mono ofensivo (Pabón Parra, 2016).

En primer término, el tipo penal revela que el comportamiento del sujeto activo, se clasifica como un delito de comisión. Esto se debe a que el autor debe

llevar a cabo una acción positiva en este caso orientada a obtener un beneficio económico mediante engaños (Arango Durling, 2023)., aplicable también a la estafa informática, que se enfoca en la manipulación informática o en el uso de artificios similares, a través de los cuales se concreta la acción delictiva mencionada.

Además, de lo anterior, el tipo penal es un delito de resultado, de daño o lesiones, ya que impacta en el patrimonio económico de una persona mediante engaños que la obligan a realizar un traspaso de dinero. En este contexto, la afectación se limita a un único bien jurídico: el patrimonio económico. Por lo tanto, este comportamiento se califica como uniofensivo, puesto que la acción ejecutada no tiene un efecto supraindividual (Guerra de Villalaz et al., 2017).

Dentro del análisis de la conducta penal, hay un elemento crucial y es la duración de la ofensa perpetrada por el agente. Al considerar el tipo penal examinado, se puede clasificar en dos categorías: los delitos de tipo instantáneo y los de tipo continuado. Los delitos instantáneos se consuman de manera inmediata, es decir, la conducta del agente se materializa en el momento en que se lleva a cabo. En contraste, los delitos continuados se manifiestan a través de múltiples acciones que, aunque diversas, persiguen un mismo resultado. En este caso, dichos comportamientos comparten una naturaleza común y están orientados hacia un objetivo singular (Arango Durling, 2018).

La estafa se ubica como un delito de ejecución instantánea, ya que se consume en el preciso momento en que la víctima realiza un acto de disposición

patrimonial a causa del engaño. Aunque el engaño puede extenderse a lo largo del tiempo, la consumación del delito se agota en el instante en que ocurre el perjuicio económico para la víctima. Es decir, cuando el autor obtiene un beneficio ilícito y la víctima experimenta una pérdida patrimonial, el delito se considera completo (Donna, 2004).

Es crucial destacar que la estafa informática presenta diferencias significativas respecto a la estafa común. En este tipo de delito, no se requiere la misma intención de engaño; engloba conductas como la creación de programas maliciosos o la manipulación indebida de datos, con el fin de obtener un beneficio económico a expensas de un tercero (Romero Soto, 1990).

3.3. Criterios doctrinales diferenciadores entre la estafa clásica o común, y la estafa informática.

La introducción masiva de computadoras desde mediados de los años ochenta ha transformado el escenario tecnológico, situando al internet como un potencial factor criminológico y herramienta para la comisión de delitos de fraudes y engaños.

Esta situación respecto a la estafa informática, o esta esta nueva forma de estafa planteó una nueva realidad, y es que la manipulación de una computadora que influya en el resultado representa un engaño, un error o un acto dispositivo. Esta interrogante generó una serie de tesis plasmadas en la doctrina(Castillo González, 2016), y también condujo también a que los países introdujeran la estafa por medios informáticos en la estafa común o convencional.

3.3.1. Tesis de la explicación de la Estafa General a la Estafa de Computadoras

Para algunos autores entre la estafa convencional y estafa informática no hay diferencias, fundamentándose en el concepto de error mediatizado por computadora. Este principio sugiere que la interacción entre humanos y máquinas puede generar errores en las decisiones de las personas, lo que a su vez puede llevar a situaciones de estafa (Javato Martín, 2008).

En este sentido, es importante señalar que la estafa convencional requiere como elemento fundamental la existencia de un engaño, la inducción al error o el mantenimiento en el mismo a través de dicho engaño. Esto afecta a la víctima, llevándola a realizar un acto dispositivo que ocasione un perjuicio patrimonial. Estos elementos sugieren que cualquier manipulación podría considerarse simplemente un error humano. Sin embargo, es necesario precisar que, en la estafa tradicional, el desplazamiento patrimonial se efectúa a través del comportamiento de la víctima.

Así, la estafa representa una forma de auto-daño, aunque esta postura carece de fundamento, ya que no se trataría de una autolesión. En esta situación, no es la persona afectada quien realiza un acto dispositivo; en cambio, el delincuente logra la transferencia patrimonial mediante manipulaciones que afectan el sistema de procesamiento de datos, resultando en información incompleta o fraudulenta (Castillo González, 2016). Siguiendo la línea de lo antes afirmado, la estafa se centra en la acción fraudulenta, es decir, en el engaño.

También en esta línea, hay que recordar que la interpretación tradicional en la estafa ha desestimado el engaño dirigido a máquinas o instrumentos. En el libro de

Mosquete (1958) sobre Antón Oneca, José: Las estafas y otros engaños, en el Código penal y en la Jurisprudencia se presenta la postura tradicional que sostiene la no posibilidad de engañar a las máquinas, argumentando que la estafa implica causar un error en otro, este otro solo puede ser una persona física capaz de tener una percepción errónea de la realidad.

Todo lo expuesto, sugiere que la estafa se establece en una relación interpersonal, donde el engaño se dirige a una persona física que debe interpretar el contenido engañoso, lo que resulta en un estado psicológico de error. Así, se evita la comprensión del engaño y la aplicación de la norma de estafa podría considerarse una analogía prohibida en contra del acusado.

A pesar de los avances en la definición de la estafa en el contexto informático, este delito sigue encuadrándose claramente en la categoría de delitos cibernéticos. Algunos autores han cuestionado esta perspectiva, argumentando que las máquinas y ordenadores no experimentan engaño ni realizan actos de disposición por error. En su lugar, simplemente ejecutan transferencias patrimoniales según las instrucciones del programador o de la institución (Gutiérrez Francés, 1990).

Antes este hecho se tiene que independientemente de la distancia temporal o de la forma en que se produzca el engaño, siempre hay una persona, aunque no sea de manera directa, que resulta afectada por el engaño. En su obra Gutiérrez Francés presenta una revisión crítica del concepto de engaño, argumentando que ha ocupado un lugar desproporcionado en el análisis. Propone enfocar la atención en las

conductas engañosas, estableciendo una conexión innovadora con el fenómeno de la estafa en la actualidad. Su razonamiento se centra en la relación causal entre el engaño, el error y la afectación patrimonial, es decir, cualquier acción destinada a inducir al error en otro. Así, la atención debe dirigirse hacia la idoneidad de tales comportamientos para provocar el error.

En concordancia con lo anterior, la estafa cometida mediante medios informáticos no reproduce la dinámica propia de la estafa tradicional. Según Montalvo (1997), las nuevas modalidades delictivas caracterizadas por su ejecución digital se desvinculan fundamentalmente del engaño y del error como elementos centrales, lo que las distingue esencialmente del tipo penal clásico. Desde esta perspectiva, las similitudes entre la estafa digital y su configuración tradicional son escasas y superficiales; por tanto, esta última resulta insuficiente como marco interpretativo o referencia analítica para comprender adecuadamente las formas contemporáneas de fraude tecnológico. (Montalvo, 1997).

En este contexto, diversos autores sostienen que la estafa informática no constituye una figura delictiva aislada, sino que mantiene una estrecha vinculación conceptual y estructural con las modalidades tradicionales de fraude. Esta perspectiva ha sido desarrollada por el jurista Ricardo Mata y Martín en su obra La estafa electrónica en los pagos de las redes de telecomunicaciones, donde detalla lo siguiente: "…*la estafa informática sigue manteniendo los elementos de la estafa genérica, es decir que la realidad de una mera adaptación Legislativa a las necesidades que incorporan la estafa informática…*" (Marin, 2007)

En atención a lo expuesto, no podemos compartir esta línea de razonamiento. La modalidad de estafa objeto de análisis no se limita a una mera conducta engañosa tradicional, sino que implica la manipulación intencional de un sistema informático con frecuencia mediante técnicas de ingeniería social con el fin de obtener, de forma ilícita, un control efectivo sobre el patrimonio de la víctima. Este tipo de control se concreta, en la práctica, en un acto de apropiación indebida de fondos realizada de forma remota y mediante medios tecnológicos. Se caracteriza por tres elementos esenciales:

- **Su naturaleza tecnológica:** opera exclusivamente a través de medios informáticos.
- **Su intencionalidad:** Implica la voluntad deliberada de eludir controles.
- **Su efecto en el patrimonio:** Provoca una perdida inmediata del patrimonio. (Morullo, 2002)

En este contexto, el elemento central y distintivo de la nueva modalidad delictiva radica en la manipulación informático en un artificio tecnológico equivalente que opera como sustituto del engaño tradicional. Dicha manipulación no solo simula una situación real, sino que induce directamente al sujeto pasivo en un error esencial, conduciéndolo, de forma inconsciente y sin consentimiento válido, a realizar una disposición patrimonial

.Es precisamente esta capacidad de generar un error funcionalmente equivalente al engaño clásico pero mediante medios digitales lo que constituye la novedad sustancial y la relevancia jurídica de la figura. Por tanto, resulta indispensable analizar con rigor el alcance y los límites de este requisito: no basta con cualquier alteración técnica; debe tratarse de una intervención que,

objetivamente, falsee el funcionamiento normal del sistema y, subjetivamente, provoque un error determinante.

Lo anterior permite concluir que esta forma de manipulación puede producirse en cualquier etapa del procesamiento o tratamiento automatizado de datos, y desde cualquier ubicación geográfica incluso fuera del territorio nacional siempre que se afecte un sistema informático protegido.

Esta flexibilidad espacial y temporal constituye una de las principales diferencias respecto a la estafa tradicional, cuyo desarrollo suele requerir una interacción directa, personal y circunscrita en el tiempo y el espacio.

Por tanto, calificar este comportamiento bajo una figura penal genérica como la estafa contemplada en el Código Penal de Panamá resulta insuficiente y conceptualmente inadecuado. Su naturaleza técnica, su dependencia de medios informáticos y su potencial escala transnacional exigen un enfoque específico: debe analizarse bajo un tipo penal especializado, que capte con precisión las particularidades del delito informático como la alteración no autorizada de datos, la interferencia en sistemas informáticos o la suplantación tecnológica y que refleje adecuadamente su gravedad, modalidades y efectos distintivos.

3.3.2. Tesis de la no aplicación de las disposiciones de la estafa general a la estafa por medios informáticos.

Esta tesis se basa en la noción del engaño en relación con un ser humano, que se da en la estafa convencional, y que no ausente en la estafa por medios informáticos, en la que además falta el error relacionado con el individuo y el acto de disposición por parte de la persona afectada, ya que tanto el error como el acto

dispositivo son elementos vinculados a la víctima. Este razonamiento se apoya en el hecho de que las computadoras no pueden ser engañadas, y tampoco cometer errores, estas no tienen la capacidad de disponer.

De acuerdo a lo expresado, podemos indicar que la estafa requiere como presupuesto de aplicación una situación fáctica psicológica, lo que se aclara por las diferencias entre el cerebro y la computadora (Castillo González, 2016). La teoría propuesta indica que los seres humanos procesan información con el objetivo de tomar decisiones que pueden modificar su entorno. Al mismo tiempo, estas personas son vulnerables al engaño. En este sentido, es crucial que se cómpreda que una computadora necesita ser operada por un ser humano para que pueda establecer un marco legal, ya que la tecnología por sí sola no actúa; necesita la intervención humana para facilitar el engaño.

En este contexto, la diferencia esencial entre la estafa tradicional y la estafa informática radica en que esta última utiliza un medio tecnológico para generar confianza en una tercera parte, y a través de este medio, se induce al error, lo que resulta en un acto perjudicial que afecta el patrimonio de la víctima.

Es importante destacar que una computadora no tiene libertad para tomar decisiones; sus elecciones están determinadas por una programación específica. La creatividad en el sentido humano no se encuentra en los sistemas computacionales. A pesar de que la inteligencia artificial puede generar resultados innovadores, sigue operando bajo directrices establecidas por sus programadores. Por lo tanto, la

inteligencia que exhibe una computadora no proviene de ella misma, sino de quienes la han diseñado y programado. Por consiguiente, se concluye que el cerebro humano cuenta con una inteligencia reflexiva, mientras que la inteligencia de los sistemas informáticos está supeditada a la programación o control que les otorgan sus desarrolladores.

Para otros autores, la no aplicación de las disposiciones de la estafa general a la estafa por medios informáticos o estafa informática, radica en el problema de las técnicas legislativas y la carencia de elementos estructurales que exige el delito de Estafa informática.

En este sentido, señala Posada Maya (2017) que estamos ante delitos automáticos, técnicos, que ocurren el ciberespacio, que no resultan comunes a los delitos físicos tradicionales, como es el caso de la Estafa común, por lo que su construcción legal debe ser autónoma precisando sus elementos desde una infraestructura informática que en su contesto determine las conductas punibles de manera que encuadre perfectamente con el principio de legalidad.

3.4. Problemática del delito de estafa informática en la legislación actual

En la era digital, la tecnología influye en casi todos los ámbitos de la vida diaria, los delitos informáticos se han convertido en una preocupación cada vez mayor para las sociedades contemporáneas. Panamá, como país en desarrollo y centro tecnológico de la región, no es inmune a esta problemática, especialmente en lo que respecta a las estafas informáticas.

El delito de estafa informática representa un reto considerable para el sistema legal en Panamá, revelando debilidades en la legislación vigente y generando dudas acerca de la efectividad en la salvaguarda de los ciudadanos y en la persecución de aquellos delincuentes que utilizan herramientas informáticas para llevar a cabo engaños en perjuicio de las personas.

La legislación en Panamá, aunque ha realizado esfuerzos para combatir los delitos informáticos, enfrenta diversas dificultades que restringen su eficacia en la lucha contra las estafas por internet. En primer lugar, el marco legal vigente, especialmente lo que se encuentra en el Título VIII del Código Penal, relativo a los delitos contra la Seguridad Jurídica de los Medios Electrónicos, presenta indicios de desactualización ante la acelerada evolución de las tecnologías y las tácticas empleadas por los ciberdelincuentes. Esta discrepancia entre la legislación y la realidad tecnológica genera vacíos legales que pueden ser aprovechados por personas con intenciones maliciosas.

Por otro lado, la definición y el alcance del delito de estafa informática o estafa por medios informáticos, en la legislación panameña es insuficiente para incluir todas las modalidades emergentes asociadas a este fenómeno criminal. Esta falta de claridad y amplitud en la tipificación del delito complica la labor de los organismos de seguridad y del sistema judicial a la hora de perseguir y procesar eficazmente a quienes llevan a cabo este tipo de conductas.

Un aspecto fundamental a considerar es la naturaleza transnacional de los delitos informáticos. La estafa a través de medios electrónicos tiene la capacidad de sobrepasar las fronteras nacionales, lo que genera importantes desafíos en cuanto a la jurisdicción y la aplicación de la ley. La legislación vigente en Panamá podría no disponer de los mecanismos adecuados para enfrentar de manera efectiva los casos que involucren a delincuentes o víctimas en varios países. Esto resalta la urgencia de fortalecer la cooperación internacional en el ámbito de la ciberdelincuencia.

La recolección, preservación y presentación de evidencias digitales representa un desafío considerable. La naturaleza efímera y compleja de este tipo de prueba exige procedimientos especializados y conocimientos técnicos que, a menudo, no están debidamente contemplados en la legislación vigente. Esto puede resultar la eliminación o mala interpretación de evidencias cruciales, lo que pone en riesgo la integridad de los procesos judiciales.

Además, la falta de formación adecuada para las autoridades judiciales y policiales en delitos informáticos agrava esta problemática. Sin el conocimiento técnico necesario, la investigación y la persecución efectiva de casos de estafa informática se complican, volviéndose en algunos casos inviables.

La legislación también debe encontrar un delicado equilibrio entre la necesidad de investigar, enjuiciar delitos y la protección de los derechos de privacidad y datos de los ciudadanos. Este equilibrio es fundamental para mantener la confianza pública en el sistema legal y en las instituciones encargadas de hacer

cumplir la ley. Por otro lado, las penas y sanciones establecidas en la normativa actual podrían no ser lo suficientemente disuasorias, sobre todo si se considera el considerable daño económico que pueden ocasionar las estafas informáticas.

Según el medio de comunicación TVN en la redacción de González (2024) se ha reportado un alarmante incremento del 113% en este tipo de delitos entre los años 2023 y 2024. Esta cifra pone en manifiesto un aumento significativo en conductas delictivas que incluyen el acceso ilegal a bases de datos, redes o sistemas informáticos, así como la apropiación, modificación y uso indebido de información, abarcando estafas y otros comportamientos ilegales.

Sumado a lo antes referido, la División de Ciberdelitos de la Dirección de Investigación Judicial, destacó que para lo que iba del año 2024 se registraron 2000 denuncias relacionada con fraudes y estafas por ventas a través de autos y terrenos por redes sociales, resaltando técnicas como el phishing, ransomware y suplantación de identidad.

Como se observa, el delito de Estafa por medios informáticos previsto en la legislación vigente no cumple con las medidas necesarias para garantizar la seguridad jurídica, facilitar la persecución y evitar la impunidad de esto hechos y cumplir con las obligaciones internacionales.

La ausencia de un tipo penal autónomo en la estafa informática, y la situación en la que el interprete se remite a las exigencias de la etapa convencional o común

n, es desacertado, según veremos más adelante, porque comprenden un fenómeno totalmente distinto, hechos que se dan a nivel personal o físico de carácter presencial, respecto a otros que se dan el línea o en el ciber espacio.

Además, de lo anterior que asimilar el delito de estafa común y estafa por medios informáticos es desacertado, porque son hechos de naturaleza diversa, con conductas o comportamientos diversos aunque tengan en común el daño patrimonial.

A efectos de lo anterior, solo hay que señalar por el momento que la Estafa por medios informáticos regulada en la actualidad, resulta un tipo legal contradictorio respecto a los pases que lo tiene regulado de manera especial, en la que se describe los comportamientos punibles de manera concreta, que deben hacer referencia al uso de la manipulación o artificio semejante, por lo que de *lege ferenda* debe constituirse como un delito autónomo.

En síntesis, los elementos estructurales de la estafa informática exigen un tipo penal específico, porque la expresión estafa por medios informáticos, es insuficiente para determinar e identificar los elementos propios de la estafa informática que es un ciberdelito con características propias y diferentes a la estafa convencional, y eso se requiere para efectos de cumplir con el principio de legalidad.

3.5. El bien jurídico protegido en la estafa por medios informáticos

3.5.1Introducción

El bien jurídico se erige como el elemento clave del tipo injusto en todo delito, ya que su afectación es fundamental tanto para definir qué conductas deben ser

sancionadas como para establecer las condiciones de dicha sanción. Este concepto se convierte en el referente principal para determinar la magnitud de la pena a aplicar, considerando dos aspectos cruciales: la relevancia del bien jurídico vulnerado y la gravedad de la infracción, que puede medirse en términos de peligro o en términos de una lesión efectiva (Galán Muñoz, 2003).

Antes de analizar el bien jurídico protegido en el caso en estudio, es fundamental comprender el concepto del bien jurídico protegido, que constituye la base esencial para salvaguardar intereses y valores fundamentales de la sociedad.

Para ahondar en la idea antes apuntada, Flores (2018,p.262) en su obra sobre Muñoz Machado, Santiago (dir.), Diccionario Panhispánico del Español Jurídico proporciona un concepto amplio en cuanto a la identidad de este concepto examinado, señalando que es una condición necesaria o al menos útil para el desarrollo de la vida de un individuo y de la sociedad". En esta misma línea, el texto ahonda en la definición penal, señalando lo siguiente:

> Cuando un bien jurídico se considera tan importante que es protegido penalmente frente a todas o ciertas formas de ataque, se denomina bien jurídico-penal. Este concepto es la base de la antijuridicidad material como lesión o puesta en peligro reprobable de un bien jurídico, lo cual es recogido por un tipo de delito como objeto jurídico de protección

Un bien jurídico se define como cualquier bien o valor que, conforme a la normativa, es considerado merecedor de la máxima protección legal. Estos bienes pueden ser de titularidad individual o colectiva y pueden clasificarse en materiales, espirituales o inmateriales (Arango Durling, 2018).

Esta explicación se alinea con el concepto que brinda Jescheck, (1999, pp. 274-275) puesto que en su libro ofrece un concepto que subsume el bien jurídico penal de manera integral. El autor indica que el bien jurídico es la base de toda interpretación de los tipos penales, ya que cumple una función sistemática con la idea de conocer la delimitación de la disposición penal. El concepto del bien jurídico es "un valor abstracto del orden social protegido jurídicamente, cuya defensa está interesada la comunidad y la titularidad corresponde a un individuo o a la colectividad"

3.5. 2 El patrimonio como bien jurídico protegido en la Estafa por medios informáticos.

En el caso del delito de estafa en general, la doctrina mayoritaria, señala que para que exista este delito, es necesario que se vislumbre un perjuicio patrimonial tangible. Esto implica que debe haber una instrumentalización de la víctima, donde su patrimonio no se vea afectado de manera directa (Balmaceda Hoyos, 2011).

Respecto al delito de estafa por medios informáticos, el bien jurídico protegido es el patrimonio, que se entiende en un sentido amplio, como el conjunto de derechos, bienes y relaciones jurídicas que puede poseer un individuo. Así, este tipo delictivo se clasifica como un delito económico de enriquecimiento con la particularidad que implica un acto de apoderamiento (Sánchez Bernal, 2009).

También la doctrina nacional ha apuntado en general, que la estafa es un delito que atenta contra la propiedad, causando un daño patrimonial a la víctima (Acevedo, 2017), y esto se extiende a la estafa por medios informáticos

Por lo que respecta, al concepto de patrimonio la Real Academia de la Lengua Española, (RAE) (s. f.) lo define, como “el conjunto de bienes pertenecientes a una persona natural o jurídica o afectos a un fin susceptible de estimación económica”. Con esto, se tiene que tanto personas físicas como jurídicas pueden tener patrimonio, siempre y cuando se cumplan las condiciones del tipo penal.

La concepción jurídica del patrimonio se refiere al conjunto de derechos patrimoniales de una persona, es decir, aquellos valores económicos reconocidos como derechos subjetivos. Desde un punto de vista económico, el patrimonio se entiende como el conjunto de valores económicos que posee una persona. Por último, la tesis mixta delimita la noción de patrimonio a los bienes y derechos patrimoniales que son económicamente evaluables y que deben ser poseídos por el sujeto en virtud de una relación reconocida por el ordenamiento jurídico (Ruiz, 2006). Lo antes mencionado comprende el concepto jurídico de patrimonio dentro del ámbito de estudio del bien jurídico protegido. La teoría jurídica del patrimonio, desarrollada por Merkel y Binding, fue la primera en intentar conceptualizar el perjuicio patrimonial como elemento del delito de estafa. Aunque inicialmente dominante en Alemania a fines del siglo XIX, fue gradualmente abandonada por la jurisprudencia y la doctrina en el siglo XX hasta convertirse en una posición minoritaria (Muñoz, 2008).

Gallego (2002) señala que Binding sostenía que el patrimonio es la suma de los derechos y obligaciones patrimoniales de un individuo. Según esta perspectiva, el

delito de estafa se manifiesta en la lesión de derechos patrimoniales ya definidos por el derecho civil o incluso el derecho público. La protección penal de la estafa depende de la existencia previa de un derecho subjetivo civil, resumido en su máxima dónde no hay derecho alguno no puede haber estafa, la concepción de patrimonio de Binding es un inventario de sus elementos, no una unidad de valor.

En el contexto de esta investigación, es crucial examinar las diversas concepciones del patrimonio, especialmente en relación con el análisis del bien jurídico asociado al delito de estafa informática. En el libro de Balmaceda Hoyos (2011) se presentan varias perspectivas sobre el patrimonio, que se pueden clasificar en económicas, mixtas, jurídicas y personales.

En el primer enfoque, el patrimonio se define como el conjunto de bienes que una persona posee y que tienen un valor monetario. Sin embargo, esta interpretación ha recibido críticas por centrarse en la pérdida económica, sin considerar el daño que esta situación puede causar. Al enfocarse únicamente en los aspectos materiales, se pierde una visión más holística del concepto de patrimonio.

El segundo enfoque, conocido como la concepción mixta, interpreta el patrimonio como un conjunto de relaciones jurídicas y patrimoniales que pueden ser valoradas económicamente. Desde esta perspectiva, es esencial tener en cuenta el acto de disposición patrimonial al evaluar el perjuicio en un caso de estafa, dado que este acto implica una responsabilidad civil. No obstante, esta concepción no presta atención al daño patrimonial en sí, ya que no aborda la situación específica,

limitándose a señalar que el perjuicio no se origina en la afectación contable del activo del titular afectado por la acción antijurídica. Por lo tanto, el análisis del patrimonio debe ser integral, evitando una visión meramente superficial.

La percepción del concepto de patrimonio según esta perspectiva se reduce a una simple acumulación de valor económico, careciendo así de la capacidad de establecer vínculos sociales. En este sentido, se desvía de la verdadera esencia del derecho penal, ya que tales enfoques tienden hacia un análisis de una economía controlada, sin considerar el aspecto del perjuicio y la responsabilidad civil que con ello se genera (Fernández, 2004).

Así, el análisis del patrimonio debe ser integral, ya que una visión meramente económica no contempla adecuadamente el daño patrimonial. Por último, la tercera apreciación sostiene que el injusto radica en la sustitución ilegal de la voluntad de la víctima que en el daño patrimonial que puede resultar de esta manipulación. Según esta noción, el propietario tiene la libertad de organizar su patrimonio, siempre que respete los límites del derecho. Por lo tanto, la estafa afecta la libre disposición de la víctima, quien al ser engañada, realiza una disposición patrimonial que no resulta ser libre (Balmaceda Hoyos, 2011).

No obstante lo anterior, considerando la dimensión de protección que representa el patrimonio en la estafa informática, y su vinculación con el fraude informático en sentido amplio, que define una forma de defraudación que se lleva a cabo a través de computadoras(Balmaceda Hoyos, 2011), mediante la manipulación

informática y que perjudica intereses económicos, no solo patrimoniales, pasaremos a continuación hacer algunas consideraciones.

En efecto la afectación del bien jurídico en la estafa por medios informáticos surge de la manipulación y el artificio informático, con la finalidad de perpetrar el acto. Por tanto, se sugiera que la acción de la estafa informática deba proteger bienes jurídicos penales autónomos, como el acceso a la información o la intangibilidad de la información, ya que la acción va encaminada a la afectación patrimonial (Rovira del Canto, 2002).

Por tanto, en el contexto específico de la estafa por medios informáticos, se salvaguarda el patrimonio como bien jurídico directamente afectado, aunque secundariamente hay otros vinculados como son de la seguridad telemática y la integridad de la información.

Y a propósito de lo anterior, debe indicarse de los riesgos informáticos y de la información, los cuales se clasifican en aquellos propios e impropios. En cuanto a los primeros, son aquellos que afectan a los datos o sus sistemas de tratamiento como nuevos bienes jurídicos penales, sin perjuicio de los que aparecen de forma secundaria; los segundos serían aquellos que afecta la información de los datos y sus sistemas de tratamiento como nuevos bienes jurídicos, aunque no son el principal objeto de la tutela penal, advirtiendo que estos son los más frecuentes.

En este concepto, el autor Rovira del Canto (2002) cree que se tiene que partir de la base de la potencialidad que estos comportamientos tienen para dañar gravemente el bien jurídico, se fundamenta en la creación de un peligro abstracto con independencia de un resultado dañino de un bien jurídico clásico. En este

sentido, dentro de la estafa informática, se debe establecer un criterio sobre este debate de posturas jurídicas que se han planteado sobre el bien jurídico, lo que lleva a debatir si el mismo es colectivo o individual.

Balmaceda Hoyos (2011) establece que “el fraude informático se entiende como una agresión al patrimonio, enfocándose en bienes jurídicos penales de carácter individual y micro social, sin considerar el impacto en bienes jurídicos colectivos de naturaleza socioeconómica” (p.141). Este planteamiento lleva a concluir que, en el caso de la estafa informática, la afectación se limita exclusivamente al patrimonio individual. Por ende, este tipo de fraude carece de cualquier afectación a bienes jurídicos colectivos, ya que la conducta del autor solo altera los bienes del individuo en el marco de una acción que se considera adecuada.

En conclusión, la acción en la estafa por medios informáticos, se traduce en una afectación al patrimonio, entendida como una disminución económica, y el hecho se consuma en el momento en que se produce el perjuicio patrimonial, y no cuando afecta un componente del patrimonio. Esto se debe a que solo tras la lesión se puede cuantificar el valor del daño ocasionado (Fernández, 2004).

Además que el delito de estafa por medios informáticos es un crimen contra el patrimonio, en este sentido, la manipulación de la víctima puede entenderse como un intento de causar lesión patrimonial, donde la materialización de esta manipulación resulta en un perjuicio concreto, y en la que se tutelan otros bienes jurídicos de manera secundaria, la seguridad telemática y la integridad de la información.

3.6. Tipo objetivo

3.6.1. Sujetos del Delito.

3.6.1.1. Sujeto activo.

El sujeto activo es la persona que realiza la conducta descrita en el tipo penal donde comúnmente el legislador lo denomina con la expresión quien. Solo la persona humana realiza la acción o la conducta descrita como punible, en la medida que tiene capacidad de realizar determinadas acciones con su voluntad consciente a lo que incluso acciona las características de imputabilidad. (Gill 2014)

Por su parte, Muñoz Pope señala que la clasificación doctrinal respecto al sujeto activo, se divide en dos tipos: aquellos que son delitos comunes, de los cuales se desprende que la acción delictiva puede ser cometida por cualquier persona, toda vez que el tipo penal no exige una cualidad específica; y otros tipos penales, delitos especiales, de los cuales se hace presente la existencia en aquellos sujetos activos con una connotación especial, de modo que nadie que no reúna tales cualidades puede ser considerado como sujeto activo de dicha infracción punible (Muñoz Pope, 2000).

Para abordar el tema de la estafa a través de medios informáticos, es crucial entender que el delito se define como una acción que infringe la normativa jurídica vigente. En este contexto, el sujeto activo es la persona que realiza la acción prohibida. La estafa en específico, implica un acto de engaño destinado a inducir a error a un tercero para obtener un beneficio económico, lo que se traduce en el desplazamiento de bienes de la víctima (Gill, 2014).

La Sala Primera de lo Penal de Argentina ha planteado un punto importante sobre el sujeto activo en el delito de estafa. Este delito se caracteriza por la intención de hacer que la víctima se deshaga de parte de su patrimonio y lo entregue de manera voluntaria al estafador para su propio beneficio. Además, se menciona que aquellos que se dedican a cometer estafas suelen actuar en grupo con el propósito de facilitar la realización de su conducta delictiva. La presencia de múltiples involucrados puede debilitar rápidamente las defensas que la víctima tiene en relación a sus bienes, lo que justifica la existencia de esta agravante, desde una perspectiva político-criminal (Caputo, 2018).

Del texto que antecede, se resaltar un tema crucial en cuanto al sujeto activo dentro de la estafa. Dentro del enfoque planteado por la corte, se sugiere que un aspecto que se debe observar es la intención del estafador al inducir a la víctima a desprenderse voluntariamente de parte de su patrimonio. Esta descripción opera como punto de partida para un análisis más profundo sobre los elementos constitutivos del delito de estafa.

Otro punto relevante a considerar es la tendencia de los estafadores a actuar en grupo o de forma coordinada. Este aspecto ofrece una perspectiva adicional para analizar el comportamiento del sujeto activo en este tipo de delitos. En muchas ocasiones, detrás de estas conductas subyace una dinámica que revela la existencia de grupos criminales organizados, que se valen de todo tipo de medios en este caso informáticos, para perpetrar el engaño.

Esta estructura grupal no solo facilita la ejecución del delito, sino que también intensifica la intervención del sujeto activo en la manipulación del artificio, en este caso, la información utilizada para perpetrar la estafa. La actuación colectiva amplifica la capacidad de los estafadores para engañar a sus víctimas, ya que permite una división de tareas más eficiente y una mayor sofisticación en los métodos empleados. Consecuentemente, este modus operandi grupal incrementa significativamente el potencial dañino del delito, justificando así su consideración como un factor agravante en el ámbito jurídico-penal.

Quienes llevan a cabo este tipo de delito, suelen contar con habilidades avanzadas en sistemas informáticos y a menudo, ocupan posiciones laborales estratégicas que les permiten acceder a información sensible. Sin embargo, también existen individuos sin relación laboral en estos campos que dominan herramientas digitales, lo que les facilita cometer fraudes (Acurio Del Pino, 2015).

Es relevante señalar que el ámbito tecnológico se ha vuelto un terreno común para la ejecución de estafas y otros delitos, debido a la accesibilidad y control que ofrecen los modernos sistemas y programas informáticos. Los perpetradores de delitos informáticos son diversos, y sus acciones varían en función de la tecnología utilizada, diferenciándose claramente de aquellos que llevan a cabo fraudes por medios convencionales. Asimismo, los autores del delito informático no son percibidos como delincuentes tradicionales; a menudo se consideran a sí mismos como individuos respetables y no enfrentan el mismo estigma social. Además, estos

delitos tienden a ser objeto de sanciones administrativas más que de penas privativas de libertad.

Es por ello que, el desarrollo intelectivo del apartado, debe iniciar señalando que las personas que cometen delitos informáticos poseen habilidades diferenciadas para el manejo de sistemas informáticos y que en muchas ocasiones su lugar de trabajo le permite acceso a una información sensible. Lo antes indicado debe tomar como referencia lo que señala el Manual de las Naciones Unidas para la prevención y control de delitos informáticos, del cual se desprende del 90% de los delitos que utilizaron una computadora o medios informáticos, conocidos por trabajadores de alguna organización, lo que la doctrina divide al sujeto activo dentro de este delito en dos apartados, Insider y outsider (13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, 2015)

Esto conduce a una realidad innegable, el uso del internet con fines delictivos ha puesto de manifiesto las vulnerabilidades inherentes a los sistemas informáticos, especialmente aquellos utilizados por instituciones financieras. Esta situación se agrava debido a la naturaleza dinámica y en constante evolución del entorno digital, donde los avances tecnológicos y las actualizaciones de software son frecuentes. Como consecuencia, el delito de estafa informática se ha vuelto más prevalente y sofisticado.

Los ciberdelincuentes aprovechan estas brechas de seguridad para explotar las debilidades de los sistemas, utilizando técnicas cada vez más avanzadas como el

phishing, el malware y los ataques de ingeniería social. Esto no solo pone en riesgo la integridad de las transacciones financieras, sino que también amenaza la confianza de los usuarios en las plataformas digitales. Además, la creciente interconexión de los sistemas financieros globales amplifica el potencial impacto de estos delitos, haciendo que la prevención y la respuesta efectiva sean cada vez más cruciales y complejas (Gemma, 2017).

El sujeto activo en los delitos informáticos presenta una diversidad de perfiles, abarcando un amplio espectro de individuos. Este rango se extiende desde expertos en informática con conocimientos avanzados hasta personas con nociones básicas de computación que no necesariamente se desempeñan profesionalmente en el ámbito tecnológico. Un fenómeno particularmente notable es la emergencia de los denominados niños genio, quienes desarrollan habilidades informáticas y conocimientos del ciberespacio de manera acelerada y autodidacta.

Estos jóvenes talentos por cuenta propia, llegan a ser capaces de ejecutar operaciones de alta complejidad técnica. En el contexto del fraude financiero informático, el sujeto activo es aquel que realiza todas las acciones descritas en el tipo penal correspondiente. Esta definición engloba desde la planificación y el diseño del ataque hasta su ejecución, incluyendo la manipulación de sistemas, la creación de software malicioso o la explotación de vulnerabilidades en las redes.

Es importante destacar que la pericia técnica no es el único factor determinante en la comisión de estos delitos. La ingeniería social y la manipulación

psicológica juegan un papel crucial, permitiendo que incluso individuos con conocimientos técnicos limitados puedan perpetrar fraudes sofisticados. Esta realidad subraya la complejidad del perfil del delincuente informático y plantea desafíos significativos para la prevención, detección y persecución de estos delitos en el ámbito jurídico y de seguridad cibernética.

Este punto lleva a abordar una cuestión controvertida desde el nivel típico de aptitudes del delincuente informático. Este tema ha generado un debate significativo en el ámbito de la ciberseguridad y la criminología. Por un lado, existe una corriente de pensamiento que sostiene que el nivel de habilidades técnicas no es necesariamente un indicador determinante en la propensión a cometer delitos informáticos. Esta perspectiva argumenta que otros factores, como la motivación o el contexto social, pueden tener un peso igual o mayor en la conducta delictiva.

En contraste, otra línea de argumentación defiende que los potenciales delincuentes informáticos son individuos con capacidades técnicas avanzadas y un profundo entendimiento de los sistemas tecnológicos. Según esta visión, la complejidad de ciertos ciberdelitos, especialmente aquellos dirigidos contra el sector financiero o sistemas de procesamiento de datos, requiere un nivel de conocimiento y habilidad técnica considerable.

Es importante destacar que esta discusión se vuelve particularmente relevante en sectores críticos como el financiero o el de procesamiento de datos. En estos ámbitos, la combinación de conocimientos técnicos avanzados con un entendimiento

profundo de los procesos específicos del sector puede resultar especialmente peligrosa si se utiliza con fines maliciosos. En última instancia, está en controversia y subraya la necesidad de un enfoque multifacético en la comprensión y prevención de la delincuencia informática que considere tanto las habilidades técnicas como otros factores contextuales y motivacionales.

3.6.1.2 Sujeto Pasivo

Sujeto pasivo es la persona natural o jurídica titular del bien jurídico vulnerado, que en la mayoría de los casos el sujeto pasivo coincidirá con el perjudicado del delito y la persona en la cual recae la acción típica. (Meini 2012)

En el caso de la estafa informática de medios financieros, el sujeto pasivo puede ser cualquier individuo o entidad cuyo patrimonio se vea afectado por engaños. En otras palabras, es la victima que se ve afectada por el sujeto activo, es decir por el proceso de apropiación ilícita de dinero depositado en la entidad financiera.

Las víctimas de estas acciones delictivas pueden incluir tanto personas naturales como instituciones bancarias y entidades gubernamentales. Todos comparten características comunes: utilizan sistemas automatizados de información, están interconectados y realizan transacciones económicas a través de operaciones informáticas. Esto los convierte en objetivos vulnerables a las estafas perpetradas en el entorno digital (Rosso, 2022).

Con el objetivo de fortalecer los supuestos previamente desarrollados, la jurisprudencia argentina ofrece un análisis significativo sobre el concepto de sujeto pasivo en el contexto de la estafa en general:

> La víctima a consecuencia del error realiza una disposición patrimonial. En efecto, debe existir un acto voluntario, aunque con vicio de consentimiento a causa del engaño y el error. La disposición patrimonial es lo esencial, porque aunque haya engaño, error o perjuicio, si no hay disposición no hay estafa y es justamente aquí donde la estafa se diferencia de los delitos de apoderamiento, cuando el sujeto pasivo voluntariamente dispone del bien, aunque con voluntad viciada (Superior Tribunal de Justicia de Córdoba, 2014).

Con base a lo expuesto, existen aspectos relevantes en cuanto al concepto del sujeto pasivo en el delito de estafa en general, desde la perspectiva del derecho argentino la jurisprudencia abordada subraya la importancia de la disposición patrimonial que la víctima realiza a consecuencia de un error inducido por el engaño. En este sentido, lo crucial en la estafa en general, es el acto voluntario de disposición de parte del sujeto pasivo del objeto material, aunque se remarca un vicio en el consentimiento a raíz del engaño y el error, que difiere de los demás delitos de apoderamiento, porque esa voluntariedad se encuentra viciada. Es por ello, que la jurisprudencia hace énfasis en este acto voluntario, aunque es producto de un engaño, singulariza el delito en cuestión, apuntando a un marco diferenciado donde el desapoderamiento es impuesto o realizado sin el consentimiento del afectado.

Este planteamiento apunta a una comprensión clara en cuanto al ámbito de la estafa y la participación del sujeto pasivo.

En cuanto al sujeto pasivo en delitos como la criminalidad informática es fundamental, ya que su identificación permite revelar los diversos ilícitos perpetrados por el sujeto activo. Sin embargo, medir la magnitud real de estos delitos es complicado, dado que muchos quedan ocultos o no se denuncian. La situación se agrava por una legislación insuficiente que protege a las víctimas, la falta de capacitación de las autoridades para realizar investigaciones efectivas y el temor de las empresas a la exposición pública y a las pérdidas económicas derivadas de una denuncia (Borghello, 2026).

También es importante destacar que el engaño dirigido al sujeto pasivo no siempre es un elemento esencial, ya que la manipulación o el artificio fraudulento intrínseco son responsables del desplazamiento patrimonial. En este sentido, no es necesario que el estafador presente un engaño directo; la alteración del patrimonio ajeno mediante manipulaciones informáticas actúa automáticamente en detrimento de un tercero. Esta realidad subraya la relevancia de la personalidad del autor, añadiendo un aspecto crucial a las condiciones jurídicas que rodean al receptor del comportamiento antijurídico (Sánchez, 2006).

3.6.1.3. Objeto Material

El objeto material se refiere a la cosa o persona que recae una acción delictiva. Otros autores, como Velásquez (2014) entienden el objeto material como la

persona o cosa material e inmaterial, sobre la que recae la acción del agente. No obstante, el autor mencionado ofrece una perspectiva más profunda en este apartado al señalar que la acción puede ser personal, como en el caso del homicidio real cuando afecta cosas, como en el hurto (cuando se trata de una cosa mueble ajena), o sobre cualquier bien, ya sea mueble o inmueble. Para fines jurídicos, es necesario abordar el objeto material desde una perspectiva más precisa, centrándonos en el patrimonio. Este aspecto del patrimonio constituye el objeto material de orden jurídico dentro del delito en cuestión.

En el caso de la estafa informática, el objeto material lo constituyen los bienes o derechos patrimoniales que son transferidos sin consentimiento a través de manipulaciones digitales. Esto incluye, el dinero en cuentas bancarias, datos sensibles y valores. La acción delictiva se centra precisamente en estos activos patrimoniales, que representan el principal objetivo de la conducta del estafador (Iberley, 2024).

Dentro de este marco, resulta fundamental considerar el patrimonio como el foco principal del objeto material. Siguiendo la idea planteada por el autor Velásquez (2014) donde la acción del agente puede ser personal o real, dependiendo de cómo se vean afectadas las distintas categorías de bienes. Sin embargo, en el caso de la estafa informática, el objeto material adquiere una dimensión particular, ya que se centra en la vulneración del patrimonio de la víctima a través de medios digitales y tecnológicos. Por tanto, entender este tipo de delito implica reconocer cómo la acción del agente puede menoscabar no solo el bien tangible, sino también activos inmateriales, afectando de manera significativa la esfera patrimonial del individuo.

Es esencial señalar que, para definir con precisión los elementos patrimoniales que pueden constituir el objeto material del delito de estafa informática, es crucial establecer una conexión clara entre el daño económico ocasionado y las alteraciones realizadas en los registros informáticos durante la comisión del delito.

En este contexto, únicamente aquellas modificaciones que impacten directamente en registros con relevancia patrimonial real pueden ser consideradas como estafa informática. Las alteraciones que no tengan esta incidencia directa en el patrimonio quedarían fuera de esta tipificación, pudiendo corresponder a otros delitos contra el patrimonio, como ocurre con la estafa convencional, o en figuras delictivas que protejan bienes jurídicos de naturaleza no patrimonial, tales como las falsedades documentales.

Para este tipo penal, los activos patrimoniales se entienden como aquellos que se representan a través de anotaciones o registros informáticos, de modo que su alteración pueda resultar en la transferencia del valor económico que encarnan a un tercero, provocando así una pérdida real de la capacidad de disposición del titular legítimo. Esta afectación debe ser efectiva y tangible, y no meramente potencial, aparente o formal.

En este sentido, la opinión de Pérez Manzano (1995) amplía la noción de activo patrimonial en el contexto del objeto material del delito. Argumenta que este concepto incluye todos los bienes o derechos que pueden ser valorados económicamente, subrayando que la condición de activo o pasivo no es intrínseca al objeto, sino que depende de la situación patrimonial del titular. Desde esta óptica, se

tiene que si un deudor transfiere su deuda a un tercero, estaría afectando un activo patrimonial del acreedor es decir, su derecho de cobro en detrimento.

3.7. Conducta Típica

Para abordar el apartado sobre la conducta típica, es fundamental definirla como la figura establecida por el legislador para valorar ciertas conductas delictivas. Esta definición se basa en una realidad predominantemente descriptiva, cuya función principal es la individualización de las conductas humanas que son penalmente relevantes (Almanza Altamirano & Peña González, 2022).

Se entiende por conducta típica, según Gill (2014,p.205) como uno de los elementos que conforma el tipo penal, que describe la acción u omisión prohibida o mandada, la cual deben someterse los asociados. Este aspecto constituye el elemento esencial o nuclear del tipo penal, el cual aparece como “el uso del verbo rector” .

Según la normativa panameña, el elemento central en el delito de estafa en general, es el *verbo rector* engañar. Este implica la utilización de maniobras que distorsionan la realidad, empleando trucos y artimañas para ocultar la verdad y manipular las circunstancias con el fin de lograr un objetivo específico (Acevedo, 2017).

De acuerdo con lo que antecede, el delito de estafa tradicional se configura con el provecho ilícito del perjuicio de otros, utilizando el engaño de ardid o la

astucia. Es fundamental destacar que el análisis jurídico que se ha llevado a cabo permite explorar a fondo la relación entre la definición típica de la estafa en su modalidad informática y las condiciones que establecen el nexo de causalidad con el resultado. En este sentido, la estafa se concretiza a través del perjuicio patrimonial causado por medio del engaño.

Los elementos constitutivos de este delito se centran en el engaño que puede manifestarse a través de maniobras fraudulentas, uso de nombres falsos, atribución de cualidades engañosas, simulación de hechos falsos o distorsión de hechos verídicos. Es fundamental que el engaño en la estafa sea de carácter trascendental; es decir, debe ser suficiente, desde las perspectivas objetiva y subjetiva, para inducir a error a otra persona (Muñoz Conde, 2015).

El error se presenta como un segundo requisito en el contexto del engaño, derivado de un comportamiento fraudulento que distorsiona la percepción de la realidad. Esto provoca que la persona engañada experimente una discrepancia entre su visión de la realidad y la realidad misma, conduciéndola a realizar una disposición patrimonial. El efecto patrimonial abarca diversas acciones, como la entrega de bienes materiales, dinero, documentos con valor jurídico o la prestación de servicios. Es fundamental que la persona que realiza esta disposición patrimonial sea la misma que ha sido engañada, lo que establece una relación clave para tipificar el delito en cuestión.

Como resultado de lo antes expuesto, se produce un perjuicio patrimonial que se traduce en un saldo negativo en el patrimonio de la víctima. Este daño es

consecuencia directa del engaño y del error, evidenciando la merma patrimonial ocasionada por el acto fraudulento. Por ende, se identifica los elementos esenciales que dan origen a la estafa, los cuales se encuentran interconectados en una progresión donde cada elemento es causa del siguiente (Mata, 2001).

Por otro lado, al analizar la conducta del delito de estafa por medios informáticos o cibernéticos, el tipo penal no establece como el sujeto activo lleva a cabo la estafa por medios informáticos, aunque se estima que la conducta puede realizarse solo por dos acciones posibles: manipulación informática y por el uso de artificio similar.

Cuando hablamos de manipulación informática Galán Muñoz (2003,p.10) indica que son:

> Aquellas actuaciones realizadas sobre sistemas informáticos que provocasen que los procesamientos de datos efectuados en ellos llevasen un resultado objetivamente defectuoso o erróneo del mismo modo que el engaño de la estafa tiene que llevar la producción de un erróneo acto de disposición patrimonial en aquel que sufre su engaño.

El concepto de manipulación informática se refiere a cualquier conducta que afecte el programa o su funcionamiento durante el procesamiento de datos, así como cualquier acción que altere los resultados de dicho procesamiento. Esta manipulación es relevante cuando busca provocar la transferencia de activos patrimoniales con el objetivo de evadir o castigar un delito.

Es fundamental definir el concepto de artificio en relación con la manipulación. Cualquier conducta que implique la intervención en sistemas informáticos y que resulte en transferencias no consentidas de activos patrimoniales debe ser catalogadas como manipulación informática. En este sentido, es evidente que todas las formas de uso o abuso de estos sistemas se basen en un simple artificio, y deben ser consideradas seriamente.

Por lo tanto, los supuestos mencionados siguen siendo relevantes en la actualidad. De estos, se extrae una mayor claridad y definición del comportamiento típico, un elemento clave en la manipulación informática, la cual, desde la perspectiva de la tipicidad tradicional, se entiende como un engaño suficiente que induce al error del sujeto pasivo o a un tercero. Es importante subrayar que en este contexto, el error que caracteriza la estafa genérica se ve reemplazado en la fórmula legal por la falta de consentimiento (Pérez Manzano, 1995).

En conclusión, toda transferencia realizada mediante manipulación informática ocasiona un perjuicio patrimonial al tercero, es un elemento fundamental en la configuración del delito de estafa informática. Este tipo de fraude genera un desbalance patrimonial que afecta al titular del bien jurídico, constituyendo aspectos esenciales para la correcta tipificación del delito en cuestión.

Como se ha señalado, la estafa se centra en la acción fraudulenta, es decir, en el engaño. No obstante, la interpretación tradicional de este delito ha desestimado el engaño dirigido a máquinas o instrumentos.

Antón Oneca (1957) destaca que no es posible engañar a las máquinas, argumentando que, la estafa implica causar un error en otro, este otro solo puede ser una persona física capaz de tener una percepción errónea de la realidad. Lo anterior sugiere que en la estafa se establece en una relación interpersonal, donde el engaño se dirige a una persona física que debe interpretar el contenido engañoso, lo que resulta un estado psicológico de error.

En ese sentido, el enfoque del engaño hay que concretarlo en la manipulación referido a acciones diseñadas para engañar a través de la utilización de herramientas digitales. La manipulación informática implica modificar elementos físicos que afectan la programación del software, lo que puede conllevar a consecuencias significativas. Acciones como hacerse pasar por un usuario autorizado para operar en su nombre con el fin de obtener beneficios, o introducir datos maliciosos para apropiarse de información sensible, son ejemplos típicos de fraudes que suelen ocurrir.

Conforme a la doctrina, la manipulación informática se define como cualquier acción del sujeto activo que interviene en un sistema informático, ya sea alterando, modificando u ocultando datos que deberían ser tratados automáticamente cambiando las instrucciones del programa. El objetivo de estas acciones es alterar el resultado final con la intención de obtener una ventaja patrimonial. Esto permite precisar mejor el concepto de estafa informática (Montalvo, 2001).

Para abordar este tema, es relevante destacar que la manipulación de datos puede ocurrir tanto en la introducción como en el tratamiento y la salida de la información. Sin embargo, un aspecto preocupante de esta manipulación es que, en la actualidad, ya no es necesario un contacto directo con el ordenador que almacena los datos. Existen tratamientos que permiten operar a distancia a través de internet o redes, lo que aumenta los riesgos asociados a la integridad de la información.

En función de lo expuesto, las principales formas en que el sujeto activo puede generar un movimiento contable a su favor son tres y se revelan de la siguiente manera:

a) Introducción de datos falsos

b) Manipulación del programa

c) Alteración del sistema de salida de datos (output)

a) **La introducción de datos falsos**: se refiere a la alteración, supresión u ocultación de información previamente ingresada en un sistema. En este contexto, no se manipula el programa en sí, sino que se modifican directamente los registros y las operaciones dentro del sistema. Aunque el programa puede seguir funcionando de manera habitual, la incorporación de datos falsos genera resultados incorrectos. Esta práctica se enmarca en la manipulación informática y puede inducir a errores significativos (Casabona & Mendoza, 2012).

a) **La manipulación en el programa** implica modificar los protocolos con el fin de beneficiar al autor, lo que a menudo incluye casos de spyware. Entre los ejemplos más comunes se encuentran los troyanos, un tipo de software malicioso que engaña al sistema haciéndose pasar por un programa legítimo o inofensivo (Gutiérrez Francés, 1990).
b) **Manipulación en el sistema de salida u output:** Se manipula en este caso el sistema de salida de datos, tales acciones pueden intervenir en el cable telefónico o modificar la impresión final. Ya que por un lado se engaña la victima para que el autor se beneficie, y por otro lado, se destruyen datos del propio sistema informático.

El análisis subjetivo lleva a comprender el concepto de artificio semejante, no se trata únicamente de manipular un sistema informático, sino de influir en otros mecanismos automáticos. Esta perspectiva se relaciona con la manipulación informática y está íntimamente vinculada a la intención del autor, así como al medio utilizado para llevar a cabo su acción dolosa de engañar a través de plataformas digitales.

En la estafa informática, la manipulación informática o el uso de un artificio semejante se lleva a cabo con el propósito de engañar y crear confusión en la víctima mediante técnicas de ingeniería social. Como señala el autor Manuel Rosso, los elementos típicos que integran este delito son: la manipulación informática o artificio fraudulento, la transferencia patrimonial no consentida por su titular, el ánimo de lucro y el perjuicio causado a un tercero.

Respecto al engaño, cabe destacar que esta nueva figura pretende proteger el patrimonio frente a los ataques propiciados por las nuevas tecnologías, descritos por el legislador como “manipulación informática o artificio semejante”. Estos mecanismos son idóneos para lograr una transferencia no consentida de activos patrimoniales, lo que constituye el acto de disposición y produce el enriquecimiento que persigue el autor.

De acuerdo con lo antes indicado, el engaño deja de ser un elemento básico e imprescindible. En su lugar, la función que antes cumplía el engaño la desempeña ahora el recurso a la manipulación informática o a un artificio fraudulento, que son los que provocan el desplazamiento patrimonial sin el consentimiento de su titular.

En cuanto al error, es relevante señalar que en la estafa informática ni siquiera se produce una relación intersubjetiva entre el autor y la víctima, ni se requiere su “colaboración” como elemento indispensable. Esto se debe a que el desplazamiento patrimonial resulta directamente de la manipulación informática. La acción delictiva no se dirige contra una persona susceptible de ser inducida a error, sino contra un programa informático que, sin incurrir en error, actúa según la información que se le suministra de manera fraudulenta. (Enrique, 2022)

En síntesis, la estafa informática representa una evolución del delito de estafa tradicional, adaptada a las realidades tecnológicas actuales. Su característica principal radica en la sustitución del engaño interpersonal por la manipulación informática o artificios técnicos, los cuales permiten una transferencia patrimonial no consentida de manera automatizada.

Esto elimina la necesidad tanto del error humano como de la interacción directa con la víctima, centrando la acción delictiva en la vulneración de sistemas informáticos. La jurisprudencia y la doctrina coinciden en que este enfoque refleja una protección legal más adecuada frente a las nuevas formas de ataque al patrimonio, donde la técnica sustituye al engaño clásico como medio de ejecución del fraude.

3.8 Tipo Subjetivo

El tipo subjetivo, se enfoca únicamente en el aspecto motivacional del sujeto que realiza la conducta prohibida. Este impulso responde a una intención de engañar, lo que se traduce en una consecuencia dolosa. Según Muñoz Conde (2015) este supuesto se relaciona con la conciencia y la voluntad de llevar a cabo los elementos del tipo penal que se estructuran en torno al dolo y la culpa.

Para Jescheck, (1999) el dolo es el núcleo central de injusto de acción en los delito y por ello puede ser caracterizado como elemento subjetivo general del tipo. Sin embargo junto al dolo ocurren a menudo elementos especiales subjetivos que parte de integrantes del tipo subjetivo y parte integrante del injusto de acción en la medida que caracteriza la acción voluntaria del autor.

Conforme a lo expuesto en el párrafo que antecede, el tipo penal consagrado en el artículo 220 del Código Penal, se observa que en la figura en cuestión es claramente dolosa. Esto no solo permite sancionar el intento, sino que incluso si es

vencible del individuo que utiliza el sistema informático en relación con los elementos de tipo objetivo, podría excluir su conducta del ámbito de la tipicidad.

La doctrina explica que un delito de comisión dolosa se define como aquel en el que la responsabilidad penal se establece mediante la realización del tipo penal. Arango Durling (2018) indica que esto implica que el sujeto debe tener la intención de provocar el resultado. Sin embargo, en los delitos es fundamental establecer la relación de causalidad para poder imputar dicho resultado.

En el contexto del delito de estafa informática, el dolo implica la intención consciente y voluntaria de engañar a otra persona mediante técnicas de ingeniería social (phishing o vishing, provocándole un daño patrimonial. Esta intención puede manifestarse de forma previa al acto delictivo o simultáneamente al mismo. Por lo tanto, el dolo que se presenta en un momento posterior resulta irrelevante para la configuración del delito de estafa (Fernández, 2004).

El ánimo de lucro no siempre es evidente en la comisión de un hecho punible y debe inferirse de las circunstancias que lo rodean (Arroyo de las Heras, 2006). La identificación de este elemento presenta desafíos para los operadores de justicia, dado que depende del contexto específico de cada caso. Además, su análisis se basa en las motivaciones del sujeto activo, lo que lo convierte en un aspecto relativo. Esta situación genera dificultades en la determinación de este componente subjetivo, ya que debe estar presente en el momento de la acción.

De acuerdo con lo expuesto, es importante señalar que el propósito debe ser directo y estar fundamentado en un aspecto económico, ya que actúa como una contraparte del daño patrimonial. En este contexto, es relevante destacar que la intención de lucro se encuentra intrínsecamente ligada al dolo, que se manifiesta con plena conciencia y voluntad, coexistiendo naturalmente con la propia falsedad. En otras palabras, se refiere al deseo o la meta de obtener un beneficio patrimonial, una ganancia que es precisa, concreta y perfectamente identificable (Balmaceda Hoyos, 2011).

En este contexto, es importante destacar que el ánimo de lucro en el delito de estafa abarca tanto el beneficio propio como el ajeno. No es necesario que el autor busque su propio y definitivo enriquecimiento para que se configure este elemento del delito. De hecho, el ánimo de lucro también se aprecia cuando la ventaja patrimonial se persigue con la intención de beneficiar posteriormente a un tercero. Dicho de otra manera, la finalidad de enriquecimiento no depende de lo que el autor planee hacer después con las ventajas patrimoniales obtenidas. Lo crucial es la intención inicial de obtener un beneficio económico, independientemente de quién sea el destinatario final de dicho beneficio.

En relación a la estafa informática, es importante señalar que presenta similitudes con la estafa tradicional, ya que ambas requieren la existencia de dolo y un provecho ilícito que causa perjuicio a terceros. En este contexto, el tipo de dolo es genérico e implica la intención consciente de obtener un beneficio injusto, ya sea para uno mismo o para otra persona, a costa del daño ajeno. Este aspecto se fundamenta en la obtención de resultados irregulares a través de procedimientos de

manipulación de datos, logrados mediante la alteración del funcionamiento del sistema informático la intervención ilícita en los datos o la información que está siendo tratada (Balmaceda Hoyos, 2011).

Es fundamental señalar que el delito de estafa informática ocurre cuando el acusado se aprovecha de una vulnerabilidad de un sistema informático con el propósito de obtener una cantidad significativa de dinero, beneficiándose de esta acción. Al evaluar la intencionalidad del individuo, es crucial considerar la magnitud del medio informático usado para causar el daño patrimonial. Esto se equipará a los efectos de la ilicitud derivada de la modificación indebida de un programa informático o de su utilización sin la autorización (Castillo González, 2016).

Es relevante aclarar que cualquier manipulación del proceso de creación electrónica en alguna de sus etapas puede obtener un beneficio económico que cause un perjuicio patrimonial a un tercero, y llevarse a cabo a través de internet o cualquier tipo de red. La hipótesis central en el análisis de este tipo penal es la manipulación informática.

En este mismo orden de ideas se destaca el Salvamento de Voto de la Magistrada María Eugenia López de fecha 8 de agosto del 2022, quien, en el núcleo de su razonamiento, aborda varios puntos relevantes que se puntualizan de la forma siguiente:

En este caso, se encuentra ante un delito de estafa. El Segundo Tribunal Superior absuelve a la encartada, argumentando que no existió intención de engañar,

ya que su actuación fue un error administrativo o de procedimiento. Sin embargo, la magistrada presentó una perspectiva diferente, señalando que sí hubo un ánimo de lucro por parte de la encartada, amparando su decisión en los siguientes aspectos.

a) Valoró la intencionalidad a partir de dos elementos científicos de carácter pericial. Los cuales concluyeron que la encartada ingresó en el sistema una carta de crédito de la empresa que no existía, con el objetivo de evitar que la persona encargada de revisar los saldos de los clientes detectara que estaban morosos.
b) La acción indicada, generó que se facturaran compras por las sumas de Sesenta y Tres Mil Novecientos Ochenta y Cinco Balboas con 78/100 (B/63,985.78) y Noventa Mil Seiscientos Siete con 58/100 (B/90,607.58), ascendiendo a un total de Ciento Cincuenta y Cuatro Mil Quinientos Noventa y Tres Balboas con 36/100 (B/154,593.36), cuentas que mantenían una morosidad entre noventa (90) y ciento veinte (120) días.
c) El sujeto activo manipuló el sistema informático de la empresa al introducir información falsa con el fin de engañar a los contables, lo que permitió que una empresa que no cumplía con los requisitos de crédito adquiriera materiales por un valor de B/154,593.36. Esto ocasionó un perjuicio, constituyendo una disposición patrimonial fruto de dicho error.

Conforme al razonamiento anterior, la Magistrada destacó tres elementos fundamentales: el engaño, el error y el acto de disposición. No obstante, el aspecto más relevante es su inclusión del ánimo de lucro en la relación de causalidad. Este

razonamiento es clave, ya que la Corte revela una realidad jurídica en la que los actos de engaño y error se entrelazan con la capacidad de la acusada para actuar de manera que beneficiara a un tercero, con quien tenía un vínculo.

Esto sugiere un ánimo de dominio en su conducta, el cual se caracterizaba por una cierta impersonalidad en la ejecución, ya que intentaba proteger su actuar a través de sus funciones y el uso de los sistemas informáticos de la empresa (Sentencia Penal de Corte Suprema de Justicia, 2022). Al concluir este análisis sobre el tipo subjetivo en los delitos de estafa, es fundamental subrayar la importancia de la intencionalidad en la configuración de estos ilícitos. La evaluación del dolo, junto con la consideración del ánimo de lucro, permite establecer un marco interpretativo sólido que distingue claramente la estafa de otros delitos o incumplimientos contractuales.

La jurisprudencia y los enfoques doctrinales mencionados, demuestran que el dolo no solo debe estar presente en el momento de la conducta delictiva, sino que debe ir acompañado de una manifestación de obtener un beneficio patrimonial, ya sea para el autor o para un tercero. Este aspecto refuerza la idea de que el ánimo de lucro es un componente inherente a la acción delictiva, resaltando la conciencia y voluntad del autor de actuar de manera fraudulenta.

En este sentido, el caso examinado en el Salvamento de Voto de la Magistrada López evidencia que, más allá de la justificación de un error administrativo, la manipulación intencionada del sistema para obtener ventajas económicas debe ser sancionada con el fin de preservar la integridad de las relaciones comerciales y la confianza en las transacciones. Así, este análisis se

convierte en un pilar esencial para la adecuada aplicación del derecho penal en el ámbito de la estafa, poniendo énfasis en la necesidad de una rigurosa evaluación de la intencionalidad del autor en cada caso particular.

En última instancia, es crucial que los operadores jurídicos adopten un enfoque crítico y detallado en la identificación del tipo subjetivo, asegurando que las sanciones se impongan únicamente a aquellos comportamientos que evidencien un auténtico ánimo de lucro y dolo. Esto no solo contribuye a una correcta aplicación de la justicia, sino que también protege los derechos de los individuos y refuerza la confianza en las instituciones.

3.9 Antijuridicidad

En este apartado, es fundamental adentrarnos en el concepto de antijuridicidad, su aproximación doctrinal y su significado en el ámbito jurídico. La antijuridicidad plantea la problemática relativa a la distinción de los comportamientos contrarios a lo dictado por las normas legales. En términos generales, lo antijurídico se comprende como aquello que se opone al derecho de lo establecido.

Para profundizar en el concepto doctrinal, es importante destacar que la antijuridicidad, en su acepción más básica, se entiende como lo opuesto al derecho o a la juridicidad. Representa una contradicción del orden jurídico a través de una acción, aunque esta definición solo es admisible desde una perspectiva semántica o gramatical.

Adicionalmente, es necesario señalar que la antijuridicidad se divide en dos categorías principales, siendo inicialmente la Antijuridicidad formal, que se centra en la contravención directa de lo dispuesto en la ley. Es decir, la conducta que viola expresamente una norma jurídica, mientras que la Antijuridicidad material se enfoca en la lesión puesta en peligro del bien jurídico protegido por la ley penal. Esta categoría va más allá de la mera contradicción con la norma y evalúa el daño real o potencial causado al interés tutelado por el derecho (Plascencia Villanueva, 2004).

Aunado a estas consideraciones, es relevante mencionar la posición doctrinal de Arango Durling (2018) quien aporta una definición más precisa y contextualizada, determinando que la antijuridicidad se define como la contrariedad que se da con el ordenamiento jurídico, es decir, cuando el sujeto realiza un comportamiento típico que contradice las normas establecidas.

La antijuricidad en el delito de estafa informática se refiere a la contradicción entre el acto cometido y las norma jurídica vigente. Cometer una estafa mediante medios informáticos implica afectar un bien jurídico protegido, que en este caso es el patrimonio económico y la seguridad de las personas. Por lo tanto, cualquier conducta destinada a engañar a la víctima a través de correos electrónicos falsificados o manipulación digital contraviene directamente las disposiciones establecidas en el Código Penal, específicamente en el artículo 220 la cual sanciona la conducta de engañar a otro con el fin de obtener un beneficio ilícito.

Expuesto lo que antecede, se indica que este delito se configura cuando el autor mediante el empleo de tecnologías de la información y comunicación, produce un engaño que lleva a la víctima a realizar un acto de disposición de su patrimonio en favor del perpetrador. En este sentido, se subraya la naturaleza antijuridica del comportamiento penal examinado, dado que vulnera principios fundamentales de orden jurídico, como lo es la protección del patrimonio y la confianza en las transacciones digitales.

Considerando lo señalado, resulta esencial explorar en profundidad las implicaciones vinculadas a la conducta ilícita y las circunstancias bajo las cuales un comportamiento antijurídico se clasifica como tal. En este sentido, Castillo González (2016,p.462) aclara que “alterar o modificar el contenido de datos o programas almacenados, así como realizar un ataque no autorizado a un sistema de procesamiento de datos en funcionamiento con el objetivo de enriquecerse.

En este sentido, lo expresado por el autor extrae que la ilicitud se encuentra en la manipulación deliberada, no autorizada y técnicamente adecuada de datos, programas o sistemas de procesamiento con el objetivo de obtener lucro, lo que se traduce en un fraude informático que causa un desvío patrimonial injustificado.

Por lo antes referido, la conducta ilegal se define por los siguientes aspectos:

i. Alteración o interferencia en la integridad, disponibilidad o confidencialidad de la información o del sistema
ii. Falta de autorización o un uso excesivo de los permisos

iii. Intención de enriquecimiento personal

iv. Una conexión causal entre la acción y el daño causado.

A partir de estos elementos, la tipificación del delito se manifiesta cuando el autor, utilizando medios informáticos, genera una falsa apariencia de legalidad o altera resultados operativos para obtener un beneficio económico en detrimento de un tercero, violando así los bienes jurídicos protegidos por las leyes penales relativas al fraude y la seguridad de la información.

Teniendo en cuenta lo mencionado, es importante señalar que un factor clave en el análisis de la antijuridicidad puede verse afectado por ciertas circunstancias que pueden justificar una conducta, como el consentimiento expreso de la víctima o un consentimiento válido. Sin embargo, en la mayoría de las situaciones, la utilización de medios ilícitos para engañar refuerza la naturaleza antijurídica del acto en cuestión.

Sin embargo, cabe señalar que la antijuricidad puede verse afectada en casos donde existan circunstancias que justifiquen la conducta, como la autorización previa de la víctima o la existencia de un consentimiento válido. Sin embargo, en la mayoría de los casos, la sola utilización de medios meramente ilícitos para engañar consolidan la naturaleza antijurídica del acto.

En este contexto, es fundamental examinar las causas de justificación y su aplicabilidad en el ámbito de la estafa informática. Sin embargo, antes de profundizar

en este tema, es necesario desarrollar el concepto doctrinal de las causas de justificación. Según el autor Gill (2014,p.289) estas son “autorizaciones o permisos otorgados por el ordenamiento jurídico que transforman una conducta típica en acorde con el derecho”

Otros autores como Almanza & Peña (2022) apuntan en cuanto a este aspecto a que las causas de justificación es lo que hubiese precedido una situación de amenaza de bienes jurídicos y que esta fuera la que impulsara la acción lesiva del autor. En el contexto del delito de estafa, las causas de justificación son excepcionales y permiten considerar lícita una conducta engañosa que, de otro modo, sería antijurídica.

Estas causas se relacionan con la legítima defensa el estado de necesidad, donde se busca proteger un bien de mayor valor, el consentimiento del afectado y el ejercicio legítimo de un derecho o deber. Sin embargo, en el caso de la estafa, estas justificaciones son sumamente inusuales, ya que este delito siempre conlleva un engaño ilegal y un deseo de lucro ilícito (Pabón Parra, 2016).

3.10 Culpabilidad

En cuanto a la culpabilidad se identifican como elementos: a) capacidad de culpabilidad, b) conocimiento de la antijuricidad y c) inexigibilidad de otra conducta.

La capacidad de culpabilidad implica que el individuo debe poseer la aptitud mental para entender las consecuencias de sus acciones, es decir, debe ser capaz de reconocer la criminalidad de su conducta. Por otro lado, el conocimiento de la

antijuricidad se considera un componente esencial de la culpabilidad según la doctrina predominante, ya que un individuo no puede ser culpable por un acto si no tenía conocimiento de que dicho acto era ilícito, lo que da lugar a la figura del error de prohibición.

En última instancia, la no exigibilidad de un comportamiento diferente se fundamenta en que, a pesar de que una persona sea imputable y reconozca la antijuricidad de sus acciones, puede actuar en violación a las normas penales. Esto ocurre porque, dadas sus circunstancias personales y el contexto en el que lleva a cabo el hecho, no se le puede exigir que actúe de otra manera (Arango Durling, 2018).

Una vez presentados los presupuestos, es fundamental analizar dos aspectos específicos: primero, la posibilidad de inculpabilidad en relación con el delito de estafa informática, y segundo, la viabilidad de la inimputabilidad en la comisión de dicho delito. Aunque la doctrina revisada no ha profundizado en este asunto, se hace referencia a las observaciones de Pabón Parra (2016) quien destacó los siguientes puntos:

- La inexigibilidad de un comportamiento diferente puede surgir de un miedo insuperable o de una coacción ajena insuperable.
- En el caso de incapacidad de culpabilidad, la inimputabilidad no es reconocida.
- La falta de conocimiento sobre la antijuricidad puede dar lugar, de manera excepcional, a un error de prohibición.

El análisis de los presupuestos previamente mencionados debe enfocarse en dos aspectos clave: las posibles formas de eximir de responsabilidad en los casos de fraude informático y la posible inimputabilidad del autor al llevar a cabo dicho delito. Dentro del primer eje se destaca la relación con las suposiciones de inculpabilidad, siguiendo las reflexiones de este autor.

La inexigibilidad de un comportamiento diferente se presenta cuando el autor actúa bajo un miedo insuperable, obediencia debida o la coacción de un tercero que resulte igualmente inquebrantable. En el contexto de la estafa informática, esto significaría que, si un individuo es obligado a participar en un fraude informático debido a una amenaza grave e inminente que limite su capacidad de decisión podría argumentarse que no se le podía exigir que actuara de otra manera. En estos casos, aunque la conducta típica se haya ejecutado, la culpabilidad podría quedar excluida debido a la falta de exigibilidad.

En segundo lugar, respecto a la inimputabilidad Pabón Parra (2016) subraya que en situaciones de incapacidad de culpabilidad no se reconoce una inimputabilidad en sentido estricto. Esto exige diferenciar entre una verdadera falta de imputabilidad, que puede derivarse de un trastorno mental serio, inmadurez psíquica significativa u otras causas que eliminen la capacidad de culpabilidad, como aquellas situaciones en las que, aunque existe una disminución de la capacidad de comprensión o autodeterminación, esta no es suficiente para eliminar completamente la imputabilidad.

En el ámbito de la estafa informática, que generalmente requiere un cierto nivel de planificación, comprensión de las herramientas tecnológicas y la capacidad de representar el engaño, la demostración de una inimputabilidad plena implica probar que la persona carecía, en el momento del hecho, de la capacidad para entender la ilicitud de su acto o para actuar conforme a esa comprensión. Si esta incapacidad no es total, se podría considerar únicamente una posible atenuación de la culpabilidad.

Finalmente, la falta de conocimiento sobre la antijuricidad de una acción puede, en ciertas ocasiones, revestirse como un error de prohibición. Esto podría presentarse en casos muy específicos dentro del delito de estafa informática, por ejemplo, si el autor debido a circunstancias particulares (como la complejidad técnica del entorno, indicaciones erróneas de superiores o la apariencia de licitud del sistema utilizado), no se da cuenta de que su comportamiento infringe una norma penal específica.

En tales situaciones, si el error de prohibición es invencible, esto podría excluir la culpabilidad, mientras que si es vencible, podría resultar en una atenuación de la misma. Sin embargo, dado el aumento de la conciencia social sobre la ilicitud de las conductas defraudatorias y el uso abusivo de medios informáticos, cualquier alegación de error de prohibición en este ámbito debe ser evaluada con rigor para que no se convierta en un medio de exoneración generalizado.

3.11. Formas de aparición del delito.

3.11.1. Consumación y Tentativa.

Se considera que un delito se consuma en el instante en que se lesiona o afecta el bien jurídico protegido. La consumación se basa en la ejecución de todas las características objetivas y subjetivas definidas en la figura delictiva correspondiente. Un delito se considera consumado cuando el hecho llevado a cabo por el autor coincide con la descripción legal del mismo.

Existen dos tipos de consumación: la formal (o concepto jurídico de consumación) y el material (o delito agotado). La consumación material se produce cuando el autor alcanza la finalidad última que pretendía obtener con su acción delictiva. El ilícito se evalúa como consumado cuando el hecho realizado coincide con lo estipulado en la norma legal.

Con base al párrafo expuesto, podemos afirmar que el delito de estafa se caracteriza por ser un delito de resultado, de lesión, de ejecución instantánea.

En otras palabras, el propio tipo penal exige que se realicen actos de disposición patrimonial que provoquen perjuicio económico. El primer aspecto a desarrollar es que este tipo penal se considera un delito de resultado. Esto es relevante porque, al llevar a cabo la conducta indebida, la persona provoca un cambio en el mundo exterior, al obtener un beneficio patrimonial que, de no haber mediado el engaño, no se habría producido. Este señalamiento lleva en abordar el aspecto de la consumación. Aunque para los efectos de la consumación no es necesario que se haya producido el correspondiente provecho (Muñoz Conde, 2015).

En función de lo planteado, el presente apartado genera su efecto cuando se ocasiona un perjuicio patrimonial, ya sea de forma total o parcial, o cuando el patrimonio se encuentra en inminente peligro a causa de las acciones del delincuente. Es fundamental que el perjuicio sea de naturaleza patrimonial.

Por lo tanto, los daños que puedan ocurrir en la computadora o en los programas, es que no resulten directamente de la afectación patrimonial. No se consideran como el perjuicio patrimonial necesario según lo estipulado en el tipo penal (Castillo González, 2016). Este enfoque se centra en la existencia de un ánimo de lucro por parte del autor del delito, quien busca obtener un beneficio económico. No es imprescindible ni obligatorio que este beneficio se materialice, ya que lo determinante es que la víctima haya experimentado un perjuicio en su patrimonio.

Esto se debe a que en la realización del acto delictivo, persiste la intención del agente de apropiarse indebidamente de lo ajeno, lo que se conoce como ánimo de lucro (Muñoz Pope, 2000). Esto conlleva a resaltar las razones por las cuales se considera que el delito de estafa informática se caracteriza por implicar, en su consumación un daño real y efectivo contra un bien jurídico específico, de manera que se produzca un menoscabo tangible en dicho bien. Este razonamiento establece la conexión necesaria entre el ánimo de lucro y la afectación, siendo este un aspecto indispensable para la ejecución del hecho punible en cuestión.

Ahora bien, dentro de la consumación se debe aclarar que la estafa informática presenta serias complicaciones en su tipificación. Se sancionan tanto los

actos preparatorios como las acciones de cooperación que ocurren después del inicio de la ejecución del delito. Por ejemplo, en el caso de proveedores de servicios que transmiten datos o identifican a los destinatarios, su participación puede darse antes de que se consuma el delito, es decir, en momentos posteriores a la generación de datos, e incluso en ocasiones, sin la complicidad del autor principal. Esto se debe a que la consumación en los delitos de estafa informática requiere el acceso a los datos para que se generé un error en el destinatario, induciéndolo a la disposición patrimonial.

Para respaldar el contexto previamente mencionado, es pertinente referirse a la jurisprudencia contenida en la STS del 30 de enero de 2001, emitida por el Tribunal Suprema de España la cual apunta lo siguiente:

> En esta sentencia se señala que la identificación de los diferentes momentos de crimines en los delitos de estafa ha suscitado, en numerosas ocasiones, dificultades interpretativas. Sin embargo, la doctrina es unánime al considerar que la consumación del delito, en términos generales, se produce cuando se han llevado a cabo todos los elementos que configuran el tipo penal y se ha generado el resultado típico; esto es, el desplazamiento patrimonial que causa un perjuicio junto con el enriquecimiento indebido del autor. Por lo tanto, la consumación se da en el momento en que el engaño logra su efecto, resultando en un detrimento patrimonial para la víctima debido al desplazamiento del activo económico obtenido por el agente (STS, 30 de Enero del 2001, 2001).

En resumen, la sentencia del Tribunal Supremo del 30 de enero del año 2001 subraya un concepto fundamental en el delito de estafa, la consumación no se limita al simple uso del engaño ni a la inducción de un error en la víctima. Se establece que la consumación ocurre cuando dicho engaño resulta en un desplazamiento real del patrimonio, generando así un daño a la víctima y un enriquecimiento indebido para el autor del delito. Solo cuando todos los elementos constitutivos (engañar adecuadamente, provocar error realizar una disposición patrimonial y ocasionar perjuicio/enriquecimiento), se puede considerar que el delito está consumado mientras no se produzca este resultado patrimonial, las acciones permanecerán en el ámbito de la tentativa.

Esta perspectiva es significativa para delitos como la estafa, ya sea en su modalidad informática o procesal, debido a que permite distinguir con claridad entre actos preparatorios, tentativa y consumación, según se haya afectado o no el patrimonio de la víctima.

Respecto a Zaffaroni et al. (2000) define la tentativa de delito como una acción que es tanto objetiva como subjetivamente típica del delito en cuestión, pero a la vez distinta. Esta distinción se debe a un dispositivo amplificador de la tipicidad que permite analizar la acción desde su inicio hasta su posible consumación. La tentativa se considera un delito incompleto, no por la falta de características estructurales, sino porque aún no se han concretado en el tiempo.

La tentativa se presenta cuando el autor, con la intención de cometer un delito específico, inicia su ejecución pero no logra consumarlo por factores ajenos a su voluntad. Esta noción abarca las tentativas idóneas, donde la acción es apta para consumar el delito, como las tentativas inidóneas, donde la acción no tiene capacidad para ello. En esencia, no hay un único delito de tentativa, sino múltiples tentativas de delitos, reflejando la proyección retrospectiva del tipo penal.

De acuerdo a lo anterior, se resalta que dentro de la estafa la tentativa es válida no obstante, en algunos casos no es posible afirmar que el engaño tenga la idoneidad para generar un error, ya que solo en ciertos casos es posible prever el delito de antemano. Para proporcionar un contexto sobre este caso, es importante mencionar lo que se expone en la sentencia del Tribunal Supremo de España, STS, 21 de octubre del 1998, (1998) se analizan diversos aspectos relacionados con la tentativa a través de una perspectiva casuística:

> Así se ha declarado estafa en grado de tentativa el caso de dos jóvenes. Abordaron a la joven M. T, enseñándole un papel con unas señas y un número coincidente con un décimo de lotería, diciéndole que el procesado Manuel, que era analfabeto, había comprado un décimo de lotería a un señor del pueblo, habiendo resultado premiado el décimo con la cifra de cuatro millones y que si se lo financiaba le daría parte del dinero, repartiéndolo también con el otro procesado. Al darse la joven cuenta del engaño e invitarles a que la acompañaran a la Comisaría, salieron huyendo: Manuel inmediatamente y el otro procesado poco después, por seguir acompañando a la joven un cierto

> tiempo para disimular. Es claro que la voluntad finalísimamente dirigida, logró, o la comisión del hecho punible perseguido, quedó objetivada por la realización de actos ejecutivos indubitados y manifiestamente idóneos y congruentes para el logro del fin delictivo perseguido, y que si no lo alcanzaron, no fue, ciertamente, porque voluntariamente desistieran de seguir por el camino del mal para retornar al buen camino, sino porque, contra su voluntad, se vieron obligados a interrumpir el iter criminis al verse descubiertos por la víctima.

El fallo analizado ilustra con claridad los criterios jurisprudenciales que permiten distinguir la tentativa de estafa y descartar la existencia de un desistimiento voluntario. El Tribunal, ha observado que los acusados no se limitaron a realizar actos preparatorios, sino que llevaron a cabo acciones ejecutivas evidentes, aptas y orientadas directamente a lograr el resultado delictivo. Se acercaron a la víctima, elaboraron un engaño concreto (el falso décimo premiado), propusieron un reparto del supuesto premio y trataron de conseguir que la joven realizara una disposición patrimonial a su favor. Sin embargo, la estafa no llegó a consumarse porque la víctima se percató del engaño y, al sugerir acudir a la Comisaría, provocó la huida de los autores. Por lo tanto, la interrupción del proceso delictivo se debió a una causa externa y contraria a la voluntad de los infractores, lo que excluye la aplicación de la excusa absolutoria que requiere una renuncia libre, espontánea y efectiva al plan delictivo. Así, la resolución reafirma que existe tentativa de estafa cuando se han realizado actos ejecutivos claros y coherentes con la intención de defraudar.

Esto, conlleva a ejemplificar una situación como el phishing, donde se envía un correo electrónico que parece provenir de una fuente legítima. En esta circunstancia, la persona ingresa sus datos, pero la transacción no se lleva a cabo, y al percatarse de que no pudo completar el proceso, el delincuente cancela la cuenta. En este caso, se observa que aunque se han cumplido los elementos del delito, el resultado final no se materializa, es decir, el perjuicio patrimonial no se produce realmente, lo que genera una tentativa dentro del comportamiento de estafa informática.

No obstante, la estafa informática presenta dos inconvenientes que en ciertas situaciones complica la identificación de la tentativa. A continuación, se analizan estos aspectos:

- La ausencia de la inmediatez temporal requerida para calificar una acción como tentativa.
- Por lo general, quienes llevan a cabo las acciones preparatorias son distintos de aquellos que realizan la copia o el plagio mediante el programa que engaña a la víctima (Corcoy Bidasolo, 2007).

En resumen, el estudio de la consumación y la tentativa en el delito de estafa, especialmente en su variante informática, revela que se trata de un delito que se define por su resultado. La consumación de este delito se requiere de la manifestación de un daño patrimonial efectivo, ya sea total o parcial que esté relacionado con la intención de lucro del delincuente y el impacto económico generado por el engaño.

Hasta que dicho resultado no se produzca, a pesar de que se hayan llevado a cabo acciones específicamente dirigidas a engañar a la víctima, la conducta se sitúa en la fase de tentativa. Este punto ha sido reafirmado por la jurisprudencia del Tribunal Supremo español de manera consistente.

La situación se complica en los casos de estafa informática, dado que la intervención de la tecnología dificulta la conexión inmediata entre el engaño y la pérdida patrimonial, y a menudo los individuos que realizan los actos preparatorios son distintos de quienes llevan a cabo el ataque de manera efectiva. Esto, requiere una minuciosa reconstrucción del proceso delictivo para poder identificar el momento de consumación y distinguirlo de los casos de tentativa punible.

3.11.2 Autoría y Participación Criminal.

Según el Diccionario del Español Jurídico, se establece que la autoría del delito es la responsabilidad por el delito en calidad de autor. Para autores como el profesor Gill (2014) señala que el concepto de autoría resulta extraño dentro de los elementos de la conducta típica, sin embargo, el mismo aproxima a una definición doctrinal destacando que la noción jurídica examinada tiene que ver con las personas que intervienen en el delito, con independencia de las cualidades de esta persona, es decir, si se trata de autores o partícipes.

En este sentido, en cuanto al concepto de participación criminal autores como Puig, (2015) indican que “alude a los sujetos que se encuentra en una posición secundaria con respecto al autor, razón por la cual que este realiza no el hecho

principal, sino un tipo dependiente de aquel" (p.422). Con lo expuesto, se indica que la participación en sentido amplio existe cuando una pluralidad de personas toman parte en la ejecución del hecho punible dentro del carácter que fuere, es decir como autores, cómplices o instigadores.

Dado lo que ha ocurrido, es fundamental entender las diferentes maneras de participación. A tal efecto, es pertinente citar un fallo de la Corte Suprema de Justicia que menciona lo siguiente:

> El autor es la persona que ejecuta la conducta descrita en el tipo penal; mientras que la coautoría se da cuando varias personas, previa celebración de un acuerdo común, llevan a cabo un hecho de manera mancomunada, en tanto que la complicidad primaria tiene lugar cuando la persona contribuye a un hecho ajeno, si cuya participación no se hubiera podido realizar el hecho punible; y la complicidad secundaria se configura cuando la participación del sujeto no es necesaria para la comisión del hecho punible, por lo cual éste se hubiera ejecutado sin su colaboración (Sala de Casación Penal, 2009).

En relación a lo mencionado previamente, se afirmar que el autor es aquel que lleva a cabo directamente el acto descrito en el tipo penal, es decir, quien ejecuta el verbo rector. Sin embargo, la Corte también reconoce otras modalidades de autoría, como la coautoría, y además establece diversas formas de participación, tales como la complicidad primaria y secundaria. Este enfoque permite una comprensión clara y razonada de las distintas maneras de involucrarse que contempla la normativa penal.

Todo esto se presenta con el objetivo de contextualizar el tema que se aborda en este apartado.

Esto resulta crucial, ya que permite identificar a los distintos sujetos que intervienen en la realización del delito, siendo la autoría la forma de actuación más activa, mientras que la participación comprende actos de carácter secundario. Existen varias teorías para definir el grado de implicación de los sujetos en la ejecución del hecho típico, pero en este trabajo se adoptará la teoría del dominio del hecho, que sostiene que los autores tienen control total sobre los actos de ejecución, en tanto que los partícipes carecen de ese poder.

Con base a lo mencionado, se afirma que la autoría no se limita únicamente a la ejecución de la conducta delictiva por parte de una sola persona. En este sentido, se refiere a la autoría individual directa, donde el individuo en cuestión tiene control total sobre todas las acciones necesarias para cometer el delito, sin depender de terceros que actúen como instrumentos. En el caso específico de estafa, esto significa que la persona lleva a cabo directamente la conducta definida en el tipo penal, engañando a la víctima y generando un riesgo que puede afectar su voluntad.

Sobre la coautoría, donde varias personas llevan a cabo acciones necesarias para perpetrar una conducta delictiva. No es necesario que todos los coautores realicen todas las acciones; lo importante es que existan roles distribuidos que contribuyan a la ejecución del delito. Asimismo, incluso si alguno de los coautores no

interviene de manera directa en la ejecución, puede ser considerado responsable siempre que tenga control sobre el hecho.

La esencia de la coautoría se basa en un consenso entre los implicados, el cual puede formalizarse antes de llevar a cabo el acto delictivo, definiendo así las funciones de cada participante, o durante la ejecución del delito a través de una aceptación implícita. Un caso común en situaciones de estafa es cuando algunas personas atraen a las víctimas utilizando trucos o manipulación, permitiendo que otros ejecuten la estafa propiamente dicha.

La inducción se refiere a la acción de motivar a otra persona a cometer un delito. En este contexto, la persona inducida actúa de manera voluntaria, mientras que el inductor únicamente ejerce un papel de impulso o incitación, sin participar directamente en la realización del delito. La pena impuesta al inducido es equivalente a la que correspondería al autor del acto, debido a su función como incitador. Por otro lado, la instigación, que se encuentra contemplada en el artículo 47 del Código Penal, también implica incitar a alguien a cometer un delito, siendo la diferencia que aquí el inductor simplemente provoca la acción; el delincuente es quien finalmente lleva a cabo el acto de forma voluntaria. La sanción para el instigador que es la misma que la del autor, dada su función de incitación.

Tal como hemos ido indicando, una de las enormes particularidades dentro del delito de estafa informática es la aparición de un tercer sujeto que se revela como pieza clave para asegurar el éxito del sujeto activo: lo llamados *muleros* que

almacenan y transmiten el dinero fruto de la manipulación informática al patrimonio del sujeto activo, quedándose a cambio el mulero con un porcentaje de esa cantidad o comisión, la consideración que tendrá de cómplice primario.

Ahora bien, en el ámbito financiero se ha indicado que el término “mula” se refiere a aquellas personas que proporcionan su cuenta bancaria para recibir dinero o mercancías obtenidas de manera ilegal. Estas mulas transfieren el dinero recibido y suelen quedarse con un porcentaje de la suma total.

En este sentido, el principal responsable del fraude conocido como phishing requiere una cuenta para gestionar de manera ilícita los fondos obtenidos. La doctrina ha destacado diversas características de estas cuentas que generan sospechas entre los investigadores. Algunas de estas características son las siguientes:

- Suelen ser cuentas ubicadas en el extranjero.
- Generalmente pertenecen a una tercera persona, comúnmente conocida como mulero.
- Se crean sociedades ficticias que simulan la existencia de una empresa con el fin de ofrecer empleos fraudulentos, utilizando cuentas bancarias de terceros que no son los principales involucrados en el esquema de la estafa.
- En muchos casos, el mulero recibe una cantidad y luego envía el resto a los autores del delito a través de servicios como Western Union o MoneyGram en efectivo, lo que dificulta el rastreo de los fondos (Castillo González, 2016).

Los muleros dentro del ámbito bajo estudio representan un apoyo fundamental para la consecución del hecho punible puesto que, sabemos que la determinación de su vinculación dentro del proceso puede estar ligada con aspectos casuísticos, sin embargo, podemos destacar que dentro de su actuar converge una intención de ánimo de lucro, que viene ligada en una colaboración eficiente y causalmente relevante en la actividad antijuridica con pleno conocimiento (Ávila, 2024).

A menudo, los muleros no son conscientes de que están participando en un fraude, lo que permite entrever aspectos de autoría mediata, ya que estos creen que actúan como comisionistas financieros. Sin embargo, están involucrados en un delito de estafa informática.

En materia de complicidad se puede mencionar la venta de programas (software) que son aptos para la comisión del delito de estafa informática. Para ello, existe una modalidad dentro de la complicidad que se conoce como precursores, software necesario para cometer los fraudes. Otras legislaciones, que atienden el fenómeno criminal de la estafa informática, es que buscan castigar a los precursores de los programas, los cuales resultan elementos esenciales para cometer los fraudes.

Se trata en concreto de programas que facilitan o son esenciales para llevar a cabo las conductas fraudulentas mencionadas. Un ejemplo de esto son los keyloggers, que son aplicaciones diseñadas para registrar las pulsaciones del teclado. Estas herramientas pueden transmitir información sensible, como inicios de sesión, contraseñas, números de cuentas o de tarjetas de crédito, a quienes buscan

perpetrar un fraude. Otro caso son los sniffers, que se utilizan para interceptar datos que están siendo enviados a través de la red. Asimismo, están los programas crackeadores de contraseñas, que intentan diferentes combinaciones de contraseñas, una tras otra, hasta encontrar la correcta.

3.12 Consecuencias jurídicas del delito.

En Panamá, el delito de estafa está establecido en el segundo libro del Código Penal, específicamente en el Título VI, que aborda los "Delitos contra el Patrimonio Económico", y en el Capítulo III, dedicado a la "Estafa y otros Fraudes". El tipo penal básico de la estafa se encuentra en el artículo 220, que establece lo siguiente:

> "Quien, mediante engaño, obtenga para sí o para un tercero un beneficio ilícito en detrimento de otra persona será castigado con una pena de prisión de uno a cuatro años. Esta pena se incrementará hasta un tercio si se comete aprovechándose de relaciones personales o profesionales, o si se realiza utilizando un medio cibernético o informático."

En este sentido debemos referirnos a la pena de la estafa informática, señalando que la conducta sancionada es de 1 a 4 años de prisión, aspecto que pone de relieve un marco punitivo ordinario dentro del cual el juez debe individualizar la pena según la gravedad del hecho, tomando en cuenta el monto defraudado, el daño causado y los antecedentes. No obstante aparte de la penalidad indicada en el tipo penal la norma cuenta con agravantes especificas.

Según el contexto mencionado, la norma establece que puede haber un aumento de hasta un tercio en dos situaciones específicas: a). Primero, cuando se aprovechan relaciones personales o profesionales (como el abuso de confianza, el

aprovechamiento de una posición de seguridad o influencia), b) o cuando se utiliza un medio cibernético o informático (incluyendo redes sociales, plataformas digitales, sistemas informáticos e internet). Este incremento de un tercio significa que el juez tiene la facultad de elevar la pena dentro del marco básico, sin exceder el nuevo límite que resulta de este aumento.

Anotado lo anterior corresponde indicar en que consiste la pena. La pena es el mal (en el sentido de privación o restricción de derechos), que prevé el legislador por la comisión de un delito para un culpable del mismo. Es por ello, que su sentido radica en su carácter retributivo, en la imposición del mal por el mal cometido. (Conde F. M., Derecho Penal Parte General , 2015, págs. 48-49).

En el caso de la estafa la pena es privativa de libertad oscilando entre los 12 a los 48 meses en su modalidad simple y aumenta un tercio en su modalidad agravada.

La pena puede considerarse relativamente baja en el ámbito de los delitos patrimoniales, especialmente al compararse con el hurto agravado o el robo. Esto se debe a que, en general, la afectación económica en estos casos ocurre sin recurrir a la violencia física, lo que permite la utilización de métodos alternativos para resolver el conflicto.

Por último, recientemente en mayo de este años, se presentó a la Asamblea de Diputados el Proyecto de Ley 277 el cual fue aprobado, pero está pendiente de sanción del ejecutivo, que pretende aumentar las penas para la estafa simple de 4 a 6 años y para la estafa agravada de 7 a 12 años.

CAPÍTULO IV. Estafa Informática en el Derecho Comparado desde la regulación y necesidad de un tipo especial en Panamá.

4.1 Introducción

La estafa informática se presenta como un grupo de actividades ilícitas que se realizan mediante el uso de la tecnología, afectando no solo a las personas, también a empresas e instituciones de todo tipo, el gran crecimiento de la era digital ha dado espacio para una diversa clasificación de fraude, como consecuencia, generó actualizaciones y cambios en varios países con respecto a su legislación, en este capítulo se mencionará leyes de algunos países, que permitirán identificar debilidades y fortalezas en relación con la legislación penal panameña.

En este sentido abordaremos la legislación penal de El Salvador relacionada con la estafa informática, presentaremos una visión comparativa de la justicia sobre delitos digitales de algunos países, así como también la regulación de la estafa informática en el Código Penal español de 1995 (art. 248.2), y en el Código Penal Alemán (art,263).

Pero antes de entrar a examinar este tema, haremos referencia brevemente a algunas cuestiones sobre el estudio y análisis del derecho tanto nacional como internacional con el fin de comprender su importancia jurídica, el profesor Gutteridge señala varias disciplinas del derecho comparado y son las siguientes:

a) **Derecho comparado descriptivo:** es el que se refiere al análisis de las variantes que se puedan encontrar entre los sistemas jurídicos de dos o más países.

b) **Derecho comparado aplicado:** es el que va más allá de la mera obtención de información del derecho extranjero y su utilidad puede ser tanto teórica, como práctica. En el primer caso puede referirse a un estudio comparativo que ayude a un filósofo del derecho a elaborar teorías abstractas que, a su vez, apoyen al historiador en el conocimiento de los orígenes y desenvolvimiento de instituciones y conceptos jurídicos. Desde el punto de vista de la práctica, el derecho comparado aplicado puede referirse a reformas jurídicas, tanto como a la unificación de derechos distintos.

c) **Derecho comparado abstracto o especulativo:** este también se designa como derecho comparado puro y utiliza el comparado para ensanchar la suma total de los conocimientos jurídicos.

4.2 Ley Especial contra Delitos Informáticos y Conexos de El Salvador.

Carranza & Hernández (2022, (pp.56-57)) exponen que se comenzó a regular los delitos en el Código penal de El Salvador para la protección económica de sus ciudadanos y ciudadanas, sin embargo, a través de los avances tecnológicos los riesgos aumentaron y surgieron nuevas formas de delinquir utilizando como medios las tecnologías de la información y comunicación TIC o lo que se conoce como informática, y para darle solución a la población y para sancionar este tipo de delitos se crea la Ley Especial Contra Delitos Informáticos y conexos en el año 2016, la cual de forma autónoma regula 57 las conductas que son constitutivas de delitos informáticos y específicamente en su Art. 10 inciso 1 regula el Delito de Estafa Informática, sancionando al mismo con prisión de dos a cinco años.

De acuerdo a lo planteado por Carranza & Hernández (2022), desde la fundación del primer código Penal en 1826, ya existía una preocupación por proteger los bienes de los ciudadanos, en esa época, la estafa se entendía de una forma en la que buscaba sonsacar el dinero ajeno y esto era castigado, las leyes se van actualizando desde el 1859, 1881 y 1904, el centro del castigo era el engaño sobre la cantidad o calidad de las cosas entregadas, se empezó a legalizar estableciendo que la sanción dependía directamente del monto económico defraudado.

Sin embargo, el Código Penal de 1974 marcó un hito porque introdujo conceptos más fuertes, no solo se trataba de entregar un objeto de mala calidad, sino de cualquier engaño que buscara un provecho injusto, el código fue primero en considerar la vulnerabilidad de la víctima como un factor para graduar la pena en el año 1998 que es el más parecido a las normas actuales, se actualizó para introducir la Estafa Agravada Art. 216, donde aparecieron las primeras leyes para la era digital, sancionando por primera vez la manipulación informática como una agravante de la estafa.

Para el año 2016, se dio un paso fundamental con la creación de la Ley Especial contra Delitos Informáticos y Conexos, esa ley otorga autonomía al delito de Estafa Informática (Art. 10), reconociendo que cuando el engaño ocurre a través de las Tecnologías de la Información (TIC), se necesita un marco legal específico para proteger con eficiencia la privacidad tecnológica.

Novoa & Carcamo (2025) mencionan que la representación legal de la estafa informática en El Salvador se encuentra en el Art. 10, allí se expone que se manipule o influya en el ingreso, el procesamiento o resultado de los datos de un sistema que

utilice las Tecnologías de la Información y la Comunicación, ya sea mediante el uso de datos falsos e incompletos, el uso indebido de datos, valiéndose de alguna operación informática, artificio tecnológico o por cualquier otra acción que incida en el procesamiento de los datos del sistema, o que dé como resultado información falsa, incompleta y fraudulenta, la cual procure u obtenga un beneficio patrimonial indebido para sí o para otro, en perjuicio patrimonial ajeno, será sancionado con prisión de cinco a ocho años.

También, hace referencias a las sanciones con privación de la libertad de ocho a diez años, si las conductas descritas en el inciso anterior se cometieren bajo los siguientes presupuestos:

- En perjuicio de propiedades del estado.
- Contra sistemas bancarios y entidades financieras, y se vieren o no afectados usuarios de los mismos.
- Cuando el autor sea un empleado encargado de administrar, dar soporte al sistema, red informática, telemática o que en razón de sus funciones tenga acceso a dicho sistema, red, contenedores electrónicos, ópticos o magnéticos.

En ambos casos estafa común y estafa electrónica, se requiere que la acción penal sea ejercitada previa instancia particular, de conformidad con el artículo 17 del Código Procesal Penal, siendo el agraviado por el delito, quien deba accionar el sistema de justicia por medio de la Fiscalía General de La República, teniendo la disposición de la acción penal durante el procedimiento.

En la tabla 5, Novoa & Carcamo (2025) muestran las comparaciones entre dos bases fundamentales de la constitución de El Salvador como lo son la estafa común Art. 215 y la Estafa Informática Art. 10, aunque ambas comparten la misma lógica delictiva sus características jurídicas cambian de acuerdo al caso, los años de condena dependen del tipo de pena jurídica, donde la estafa informática cuenta con más años de condena, debido a que dicho país le ha dado una gran importancia a la tecnología, mediante los grandes avances de la ciencia una estafa informática puede robar información suficiente para destruir sistemas enteros y grandes cantidades de dinero electrónico.

En lo que respecta al fraude informático es calificado como una de las tipologías del cibercrimen en el que se da la defraudación mediante la utilización de un sistema informático como medio para transferir de forma virtual activos patrimoniales a favor del autor o de un tercero, además, se denomina diversamente como: estafa telemática, estafa por computación (Alemania), estafa informática (España, El Salvador), fraude informático (Costa Rica, El Salvador)

. En la LEDIC salvadoreña se tipifican los delitos de Estafa Informática (Art. 10) y Fraude Informático (Art. 11), en ambas figuras se observan elementos descriptivos y normativos similares en su redacción, y dicen lo siguiente:

Estafa informática Art. 10

> El que manipule o influya en el ingreso, el procesamiento o resultado de los datos de un sistema que utilice las Tecnologías de la Información y la Comunicación, ya sea mediante el uso de datos falsos e incompletos, el uso indebido de datos y programación, valiéndose de alguna operación

informática, artificio tecnológico o por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial indebido para sí o para otro, será sancionado con prisión de dos a cinco año. (p.40)

Fraude informático Art 11:

El que por medio del uso indebido de las Tecnologías de la Información y la Comunicación, valiéndose de cualquier manipulación en sistemas informáticos o cualquiera de sus componentes, datos informáticos o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas que produzcan un resultado que permita obtener un provecho para sí o para un tercero en perjuicio ajeno, será sancionado con prisión de tres a seis años".

A continuación pasamos a presentar un cuadro sobre el análisis comparativo entre estafa común y estafa electrónica.

Tabla 5. Análisis comparativo entre estafa común y estafa electrónica.

Elementos del tipo penal	Estafa común del artículo 215 del código penal	Estafa informática del artículo 10 de la ley de delitos informáticos
Elementos y objetivos del tipo penal	Uso de ardid o cualquier medio engañoso para sorprender la buena fe de la víctima o de un tercero	Manipulación, influencia en el ingreso o procesamiento de un sistema tecnológico mediante el uso indebido de datos y programación o cualquier otra acción fraudulenta que incida en el procesamiento de datos o dé como

		resultado información falsa.
Elementos normativos del tipo penal	Provecho injusto en perjuicio ajeno si la defraudación es superior a doscientos colones o su equivalente en dólares	Beneficio patrimonial indebido para sí o para otro, en perjuicio patrimonial ajeno. Sin establecer cuantía mínima
Elementos subjetivos de los tipos penales	El tipo penal es eminentemente doloso, requiere conocimiento de la ilegalidad que se está cometiendo y la voluntad de ejecutarla	Se trata de un delito doloso, donde el hecho no solo tiene conocimiento de la ilicitud de su actuar, sino un conocimiento informático necesario para la ejecución del delito.
Consecuencia jurídica	Pena de prisión de dos a cinco años en el tipo básico y de cinco a ocho años en su modalidad agravada.	Pena de prisión de cinco a ocho años en el tipo penal simple y de ocho a diez años en modalidad agravada.

Fuente: Novoa & Carcamo (2025).

En la tabla 6 Sánchez et al. (2025) que más adelante señalamos, se enfatizan una recopilación de los desafíos más importantes en la responsabilidad penal por manipulación digital en los cinco países estudiados. Observa que, a pesar de que todos los países abordados cuentan con marcos legales específicos, las sanciones y clasificaciones difieren dependiendo de la gravedad y el impacto del daño, y cada nación enfrenta la actualización de sus legislaciones, la especialización de los operadores judiciales y la protección real de los derechos digitales.

Tabla 6. Visión comparativa de la justicia sobre delitos digitales.

País	Norma Principal	Conductas Tipificadas	Penas	Desafíos y Limitaciones
Ecuador	COIP (Art. 190, 211, 234, 166).	Fraudes, acceso ilícito, suplantación, ciberacoso.	1-3 años de prisión; penas que en muchos casos configuran sanciones insuficientes o ambiguas.	Reformas urgentes, vacíos normativos, cooperación internacional.
Perú	Ley 30096, DL 1591, Código Penal.	Fraude informático, suplantación, abuso de dispositivos tecnológicos.	1-9 años de prisión y multas.	Actualización constante, especialización fiscal, adherencia Budapest.
Venezuela	Ley Especial Contra Delitos Informáticos, Ley Infogobierno.	Oferta engañosa, falsificación documentos, fraude y suplantación de identidad.	3-6 años de prisión y multas; agravantes.	Protección integral, sanciones diferenciadas y digitalización judicial.
Colombia	Cód. Penal, Ley 1273/2009, Ley 1581/2012.	Interceptación de datos, daño informático, robo y sabotaje digital.	3-8 años de prisión y multas.	Brechas legales, protección privacidad, adaptación constante a las nuevas tecnologías.
México	Código Penal Federal (reformas nuevas).	Violencia digital, suplantación, deepfakes, fraude, IA.	Sanciones proporcionales, aún en revisión.	Tipificación insuficiente, retos IA, derechos fundamentales.

Fuente: Sánchez et al. (2025).

4.3 Los Códigos Penales Español (1995) y Alemán.

En España, el Código Penal (1995), en el **libro II, título XIII, capítulo IV, en su sección 1ª** se regula el delito de estafa, en el artículo 248 que dice así:

*«*Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.

Los reos de estafa serán castigados con la pena de prisión de seis meses a tres años. Para la fijación de la pena se tendrá en cuenta el importe de lo defraudado, el quebranto económico causado al perjudicado, las relaciones entre este y el defraudador, los medios empleados por este y cuantas otras circunstancias sirvan para valorar la gravedad de la infracción.

Si la cuantía de lo defraudado no excediere de 400 euros, se impondrá la pena de multa de uno a tres meses, salvo si concurriere alguna de las circunstancias del artículo 250. No obstante, en el caso de que el culpable hubiera sido condenado ejecutoriamente al menos por tres delitos de la misma naturaleza, comprendidos en este capítulo, y siendo al menos uno de ellos leve, se impondrá la pena prevista en el párrafo segundo del presente artículo. No se tendrán en cuenta los antecedentes penales cancelados o que debieran serlo».

Respecto a la estafa informática aparece en el artículo 249 tras la reforma penal

Ley Orgánica 14/2022, de 22 de diciembre que dice así:

1. También se consideran reos de estafa y serán castigados con la pena de prisión de seis meses a tres años:

a) Los que, con ánimo de lucro, obstaculizando o interfiriendo indebidamente en el funcionamiento de un sistema de información o introduciendo, alterando,

borrando, transmitiendo o suprimiendo indebidamente datos informáticos o valiéndose de cualquier otra manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.

b) Los que, utilizando de forma fraudulenta tarjetas de crédito o débito, cheques de viaje o cualquier otro instrumento de pago material o inmaterial distinto del efectivo o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero.

2. Con la misma pena prevista en el apartado anterior serán castigados:

a) Los que fabricaren, importaren, obtuvieren, poseyeren, transportaren, comerciaren o de otro modo facilitaren a terceros dispositivos, instrumentos o datos o programas informáticos, o cualquier otro medio diseñado o adaptado específicamente para la comisión de las estafas previstas en este artículo.

b) Los que, para su utilización fraudulenta, sustraigan, se apropiaren o adquieran de forma ilícita tarjetas de crédito o débito, cheques de viaje o cualquier otro instrumento de pago material o inmaterial distinto del efectivo.

3. Se impondrá la pena en su mitad inferior a los que, para su utilización fraudulenta y sabiendo que fueron obtenidos ilícitamente, posean, adquieran, transfieran, distribuyan o pongan a disposición de terceros tarjetas de crédito o débito, cheques de viaje o cualesquiera otros instrumentos de pago materiales o inmateriales distintos del efectivo".

"Las acciones delictivas, que con anterioridad se limitaban a la "*manipulación informática o utilización de artificio semejante*", han visto ampliado su ámbito a otras conductas como *interferir indebidamente en el funcionamiento de un sistema de información; introducir, alterar, borrar, transmitir, o suprimir indebidamente datos*

informáticos de manera que se consiga una transferencia indebida de cualquier activo patrimonial en perjuicio de otro. Como ejemplo práctico de esta amplitud de términos, ahora tendría cabida en este supuesto la utilización indebida de claves para acceso a la banca online obtenidas ilícitamente (sin manipulación informática, se entiende), cuestión que con anterioridad tenía mejor encaje en una apropiación indebida" Bilbao Lorente. El delito de estafa informática https://www.barrilero.com/el-delito-de-estafa-informatica/

En cuanto al Código Penal Aleman, se regula en el artículo 263ª bajo el acápite estafa por computador, que dice así::

> "Quien con el propósito, de procurarse para sí o para un tercero una ventaja patrimonial antijurídica, en la medida en que él perjudique el patrimonio de otro, por una estructuración incorrecta del programa, por la utilización de datos incorrectos o incompletos, por el empleo no autorizado de datos, o de otra manera por medio de la influencia no autorizada en el desarrollo del proceso" (p.35).

Del examen de ambas regulaciones se observa que el concepto y alcance de estafa informática es más amplio y preciso, en la legislación penal española, y restringido en el Código Penal Alemán.

En Alemania, en cambio, el fraude informático se regula como un delito autónomo en el § 263a del Código Penal. Esta norma tipifica específicamente la obtención de una ventaja patrimonial *mediante la manipulación de datos* o *mediante la inducción al tratamiento de datos erróneos*. A diferencia del modelo español, aquí el elemento técnico la intervención sobre la integridad, disponibilidad o autenticidad de los datos o procesos informáticos constituye el núcleo del tipo, no un

mero medio. Esta autonomía permite una aplicación más precisa del derecho penal a la realidad digital, al desvincular el delito de los esquemas psicológicos del engaño tradicional y centrarse en la vulneración técnica del sistema

4.4. Especial consideración al Convenio de ciberdelincuencia de Budapest

Tenorio (2018) menciona que el 23 de noviembre del año 2001, en la ciudad de Budapest se suscribe el Convenio de Ciberdelincuencia, quedando abierto para su firma a los Estados miembros del Consejo de Europa, como también para aquellos países que, sin formar parte de este, quisieran adoptar la normativa contenida en él.

El Convenio, completa tratados existentes en el Consejo de Europa en función de cooperación en materia penal, con el propósito de mejorar la eficacia de las investigaciones y procedimientos penales relativos a delitos cometidos a través de la Red y las pruebas que evidencien la culpabilidad con el objetivo de llevar a juicio. Algunos de los artículos implementados son:

- **Artículo 2. Acceso ilícito**: Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a todo o parte de un sistema informático. Las Partes podrán exigir que el delito se cometa infringiendo delictiva, o en relación con un sistema informático conectado a otro sistema informático.

- **Artículo 3. Interceptación ilícita**: Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima por medios de técnicos de datos informáticos en transmisiones no públicas dirigidas a un sistema 43 informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos elementos informáticos. Las Partes podrán exigir que el delito se cometa con intención delictiva o en su relación con un sistema conectado a otro sistema informático.

- **Artículo 4. Ataques a la integridad de los datos**:

  I. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno todo acto deliberado e ilegitimo que dañe, borre, deteriore, altere o suprima datos informáticos.

  II. Las partes podrán reservarse el derecho a exigir que los actos definidos en el párrafo 1 comporten daños graves.

- **Artículo 5. Ataques a la integridad del sistema**: Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción,

transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.

- **Artículo 6. Abuso de los dispositivos**:
    1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

        a. La producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de:

            I. cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para comisión de cualquiera de los delitos previstos en los artículos 2 al 5del presente Convenio
            II. una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático, Con la intención de que sean utilizados para cometer cualquiera de los delitos contemplados en los artículos 2 a 5

        b. La posesión de alguno de los elementos mencionados previamente para intentar cometer un delito del art. 2 al 5.

2. No se interpretará que el presente artículo impone responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, difusión o cualquier otra forma de puesta a disposición mencionada en el párrafo 1 no tenga por objeto la comisión de uno de los delitos previstos de conformidad con los artículos 2 al 5 del presente Convenio, como en el caso de las pruebas autorizadas o de la protección de un sistema informático.

3. Las Partes podrán reservarse el derecho a no aplicar el párrafo 1 del presente artículo, siempre que dicha reserva no afecte a la venta, distribución o cualquiera otra forma de puesta a disposición de los elementos mencionados en el inciso 1 a) ii) del presente artículo.

- **Artículo 7. Falsificación informática**: Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la introducción, alteración, borrado o supresión deliberada e ilegítima de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles o inteligibles directamente. Las Partes podrán exigir que exista una intención dolosa o delictiva similar para que se considere que existe responsabilidad penal.

- **Artículo 8. Fraude informático**: Las Partes adoptarán las medidas legislativas o de otro tipo que resulten necesarias para tipificar como delito en

su derecho interno los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante:

a. La introducción, alteración, borrado o supresión de datos informáticos.
b. Cualquier interferencia en el funcionamiento de un sistema informático, con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.

El Convenio de Budapest sobre el Cibercrimen constituye un marco jurídico internacional clave para enfrentar los delitos cometidos mediante tecnologías digitales. No solo establece definiciones comunes y armonizadas de conductas ilícitas como el acceso no autorizado a sistemas informáticos, la interceptación de datos, la falsificación informática y el fraude digital, sino que también facilita la cooperación transnacional: desde la obtención de pruebas electrónicas hasta la coordinación de investigaciones entre países.

Su adopción fortalece la capacidad de los Estados para prevenir, investigar y sancionar eficazmente los delitos que afectan la economía, la seguridad de la información y la confianza ciudadana en los servicios digitales.

En el caso de Panamá, incorporar estos estándares internacionales adaptándolos de forma coherente al ordenamiento jurídico nacional no es una opción, sino una necesidad urgente. La creciente incidencia de estafas realizadas a través de medios informáticos (como el phishing, el suplantación de identidad digital

o el fraude en plataformas financieras en línea) exige respuestas ágiles, técnicamente fundadas y jurídicamente sólidas. Para lograrlo, resulta indispensable:

- fortalecer las políticas públicas en ciberseguridad y justicia digital;
- capacitar de forma continua a jueces, fiscales, policías y peritos en investigación cibernética;
- y promover mecanismos ágiles de cooperación internacional, especialmente en la preservación y entrega de pruebas electrónicas.

Solo así Panamá podrá garantizar una protección efectiva a las víctimas y construir un sistema de justicia digital capaz de responder con especialización, eficiencia y respeto al debido proceso ante los desafíos del delito informático.

4.5. Necesidad de Propuesta de un tipo penal especial de estafa informática, desde el Derecho Comparado

Luego de haber examinado el derecho comparado y el análisis doctrinal comparado, definitivamente que hay rasgos diferenciadores respecto a la regulación penal de la estafa informática en nuestro país.

Se observa que la legislación penal vigente es insuficiente y deficiente en la actualidad, y que por tanto hay una necesidad imperiosa de crear un tipo penal autónomo que regule específicamente la estafa informática, debido que en la actualidad se utiliza una modalidad agravada dentro del tipo general de estafa en el artículo 226 del Código Penal.

En comparación con otros países como España o Alemania, la estafa informática es un tipo penal autónomo con una estructura definida, mientras que en

nuestro país para la configuración de la estafa por medios informáticos, hay que recurrir a la estafa tradicional.

En el caso de España, se sancionan conductas en las que el engaño no se produce mediante medios convencionales como la mentira verbal o la falsificación documental, sino a través de intervenciones directas sobre sistemas digitales: por ejemplo, la alteración no autorizada de datos, la suplantación de identidad en entornos virtuales o la interferencia en procesos automatizados de pago. Para que la conducta sea punible, debe producir, de forma directa o mediata, una transferencia patrimonial no consentida y un perjuicio económico efectivo para la víctima

Y que los elementos estafa convencional son el engaño, error y disposición patrimonial se realiza de manera presencial y visible en relaciones interpersonales, mientras que en la estafa informática los daños y las estafas en su mayoría se realizan de manera anónima, oculta e inesperada, simplemente por la manipulación técnica del sistema, lo que genera problemas de interpretación y potencial impunidad, daños que a nivel informático son irrecuperables, dejando diversas consecuencias en la sociedad a nivel de estafa y robo, donde se requieren de pruebas contundentes sin la capacidad tecnológica para encontrarlas de manera eficiente.

La estafa informática en nuestro país es un delito por medios informáticos, es decir, un delito en la que la estafa se realiza por medios de la computadora o por medios cibernéticos y que ocurre en el ciberespacio, distinto a lo previsto en el derecho comparado.

La problemática de ser un delito por medios informáticos, según se observa de lo antes examinado, es que se analiza e interpreta la estafa informática con las

mismas particularidades del delito de estafa, lo cual es riesgoso porque con ello se puede incurrir en la impunidad o en la violación del principio de legalidad. Esto es desacertado porque son fenómenos totalmente distintos, el primero se da a nivel personal físico o de carácter presencial, respecto a la estafa informática, que se dan en línea o en el ciber espacio. Eso conduce a una inseguridad jurídica porque son hechos, en el caso de la estafa informática con determinadas peculiaridades tecnológicas, aunque tengan en común el daño patrimonial, y son realizadas de manera dolosa.

En conclusión, del estudio del derecho comparado, por el momento la estafa por medios informáticos regulada en la actualidad, resulta un tipo legal complejo y contradictorio respecto a los países que la tienen regulada de manera específica, en la que se describen los comportamientos punibles de manera concreta, que deben hacer referencia al uso de la manipulación o artificios semejante, por lo que la lege lerenda debe constituirse como un delito autónomo.

CONCLUSIONES

En este trabajo de investigación se determinó que Panamá tiene un reto considerable por adaptarse a los estándares internacionales en materia de ciberdelitos, como sucede con la estafa por medios informáticos.

No obstante, una revisión al Código Penal panameño revela que se han hecho intentos para adecuar la legislación al Convenio sobre Ciberdelincuencia (2001), entre ellos incorporando delitos por medios informáticos, como sucede con el delito estudiado.

Se ha apreciado que la estafa y estafa por medios informáticos tienen elementos comunes como es el bien jurídico protegido y el objeto material, son delitos de resultado de lesión, de ejecución instantánea y de carácter mono ofensivo, y que se clasifica como un delito económico de enriquecimiento, en la que el agente realiza este hecho de manera dolosa.

Pero también, resaltan diferencias, ya que mientras que la estafa genérica se configura con base en tres elementos esenciales el engaño, el traspaso patrimonial y el nexo causal entre ambos, su variante especializada, la estafa informática o cibernética, se caracteriza por la focalización deliberada en la manipulación de medios digitales: sistemas informáticos, plataformas en línea, redes sociales e, incluso, herramientas de inteligencia artificial. En este contexto, el engaño no se limita a interacciones personales o documentales tradicionales, sino que se ejecuta mediante técnicas sofisticadas que explotan vulnerabilidades tecnológicas y cognitivas del usuario, con el fin de obtener indebidamente un beneficio patrimonial.

También en este estudio se han identificado las tipologías y las formas de estafa más comunes en las que se destacan las siguientes: Pishing, Pharming, Carding, Vishing o Smishing, que se han denunciado en nuestro país.

De igual forma, se comprueba que la transformación legal de la estafa por medios informáticos, implica un desafío normativo real, para efectos de garantizar una tutela efectiva del patrimonio económico al sujeto pasivo de la estafa informática, en entornos cada vez más globalizados y tecnológicamente avanzados.

Por lo anterior, se propone la regulación autónoma del delito de estafa informática ya que con ello se cumpliría a cabalidad con el principio de legalidad y de tipicidad, dado que los ciberdelitos o delitos informáticos, en concreta en la estafa

informática, deben tener una estructura lógico-funcional que describa los comportamientos punibles de manera precisa. Tales comportamientos deben hacer referencia a los elementos estructurales básicos, como son el uso de manipulación informática y artificios semejantes , sin dejar de mencionar los móviles económicos, el perjuicio patrimonial, y la transferencia patrimonial no consentida situación que no ocurre en la actualidad y que dificulta su interpretación y aplicación de la ley.

En consecuencia, con la configuración autónoma de la estafa informática se garantiza la seguridad jurídica, se facilita la persecución penal y se evita la impunidad de estos hechos, al igual que se da cumplimiento al Convenio sobre Ciberdelincuencia de 2001.

RECOMENDACIONES

Proponer el delito de estafa informática como delito autónomo con una estructura lógica normativa que se adecue a los criterios de política criminal moderna, cumpla con el principio de legalidad, eliminando las interpretación en base a la estafa convencional que tiene rasgos y elementos diferenciadores, a fin de dar también una

respuesta efectiva, proporcional y previsible a las modalidades delictivas emergente, en la que debe cumplirse con los requisitos siguientes:.

- Especificidad objetiva: definir con claridad los elementos materiales por ejemplo, la utilización dolosa de medios informáticos para inducir a error a una persona o sistema automatizado encargado de procesar datos con relevancia jurídica (como plataformas de contratación electrónica, sistemas de pago sin contacto o interfaces de identificación digital);
- Criterio de relevancia técnica: incorporar la noción de *interferencia significativa en la integridad del proceso de toma de decisión informada*, ya sea en el sujeto humano o en el sistema automatizado, sin limitarse a la mera "falta de veracidad" en la comunicación; y
- Graduación objetiva de la pena: articulada no solo al daño patrimonial causado, sino también a la gravedad de la vulneración del principio de confianza en la seguridad del entorno digital entendida como bien jurídico colectivo protegido.

En segundo lugar, promover la educación digital a todos los ciudadanos en todos los niveles, y promover la capacitación de los profesionales del derecho y operarios jurídicos en tecnología para realizar sus funciones con eficiencia, evitar la impunidad y evitar los riesgos de los delitos de estafa informática y ciberdelitos en general.

En tercer lugar, Implementar una normativa que obligue a las instituciones financieras a tener sistemas altamente capacitados para detectar cualquier intento de ataque

cibernético o actividad irregular en el sistema, utilizando la inteligencia artificial como un arma indispensable, y responsabilizarse por los daños a terceros, aplicado para los sectores públicos y privados.

BIBLIOGRAFÍA

Acevedo, J. R. (2017). *Derecho penal especial: Títulos I al VII*. Imprenta Aeticsa.

Acurio Del Pino, S. (2015). *Delitos Informáticos: Generalidades* [Recurso electrónico]. s.e.

Ahmad, I., Khan, S., & Iqbal, S. (2024). Guardians of the vault: Unmasking online threats and fortifying e-banking security, a systematic review. *Journal of Financial Crime*, *31*(6), 1485-1501. https://doi.org/10.1108/JFC-11-2023-0302

Almanza Altamirano, F., & Peña González, Ó. (2022). *Teoría del delito: Manual práctico para su aplicación en la teoría del caso (doctrina, casos prácticos, esquemas y gráficos, jurisprudencia sobre temas desarrollados en los capítulos)* (2 ed). Círculo de Escritores.

Arango Durling, V. (2023). Estafa de consumo, de servicios o defraudación de servicios o alimentos, en *Boletín de Ciencias Penales* No. 20, Julio-Diciembre, 41-70.

Arango Durling, V. (2018). *Derecho Penal. Parte General.* Ediciones Panamá Viejo.

Arenas Nero, O. A. (2021). El delito de estafa en Panamá. *Visión Antataura*, *5*(1), 108-127.

Arroyo de las Heras, A. (2006). Los delitos de temeridad manifiesta y consciente desprecio por la vida de los demás en los artículos 381 y 384 del Código penal. *Estudios jurídicos*, (2006). https://dialnet.unirioja.es/servlet/articulo?codigo=4098562

Ávila, V. (2024). *Las mulas bancarias y su papel en las estafas informáticas | E&J*. LOGO-ECONOMIST-JURIST. https://www.economistjurist.es/articulos-juridicos-destacados/las-mulas-bancarias-y-su-papel-en-las-estafas-informaticas/

Ávila-Niño, F. Y. (2023). Ransomware, una amenaza latente en Latinoamérica. *InterSedes*, *24*(49), 92-119. https://doi.org/10.15517/isucr.v24i49.50765

Ayu Prado, J. E. (2017). *Sentencia Penal de Corte Suprema de Justicia (Panama), 2ª de lo Penal, 27 de Noviembre de 2017*. vLex. https://vlex.com.pa/vid/expediente-192-13c-corte-747957721

Balmaceda Hoyos, G. (2011). El delito de estafa informática en el derecho europeo continental. *Revista de derecho y ciencias penales: Ciencias Sociales y Políticas*, (17), 111-150.

Borghello, C. (2026). *Legislación y Delitos Informáticos—El Delincuente y la Víctima*. Segu-Info. https://www.segu-info.com.ar

Calle Rodríguez, M. V. (2007). El delito de estafa informática. *La ley penal: revista de derecho penal, procesal y penitenciario*, (37), 40-56.

Callegari, O. (2022). *Delitos informáticos: Pharming*. rnds. http://www.rnds.com.ar/articulos/031/RNDS_176W.pdf

Caputo, L. J. (2018). La nulidad es el único remedio procesal contra un laudo arbitral. Su alcance restrictivo también alcanza al Estado (clarificaciones de un caso argentino). *Arbitraje*, *11*(3). https://doi.org/10.19194/arbitrajeraci.11.03.10

Carranza Santos, J. H., & Hernández Guandique, D. A. (2022). *El delito de estafa informática en El Salvador* [Trabajo de Grado, Universidad del Salvador]. https://hdl.handle.net/20.500.14492/24169

Carrillo, M. R. (2013). Los desafíos del derecho penal frente a los delitos informáticos y otras conductas fraudulentas en los medios de pago electrónicos*. *Revista IUS*, *7*(31). https://doi.org/10.35487/rius.v7i31.2013.27

Casabona, C. M. R., & Mendoza, F. F. (2012). *Nuevos instrumentos jurídicos en la lucha contra la delincuencia económica y tecnológica*. Comares. https://dialnet.unirioja.es/servlet/libro?codigo=543513

Castillo González, F. (2016). *La estafa informática*. Editorial Jurídica Continental. http://sistemabibliotecario.scjn.gob.mx/sisbib/2017/000289393/000289393.pdf

Chavarría Mendoza, C. A. (2019). La importancia de la fundamentación del recurso de casación .*Iustitia Socialis*, *4*(1), 107-123. https://doi.org/10.35381/racji.v4i1.542

Colina Moreno, M. I., & Larios Rodríquez, L. Á. (2024). *La tipificación del phishing, smishing y vishing como defraudación en base a la concepción del bien jurídica seguridad informática.* [Trabajo de Grado, Universidad Nacional Pedro Ruiz Gallo]. https://repositorio.unprg.edu.pe/handle/20.500.12893/13140?show=full

Comisión Federal del Comercio. (2022). *Lo que hay que saber sobre las estafas de romances*. Consumer Advice. https://consumidor.ftc.gov/articulos/lo-que-hay-que-saber-sobre-las-estafas-de-romances

Corcoy Bidasolo, M. (2007). Problemática de la persecución penal de los denominados delitos informáticos: Particular referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos. *Eguzkilore: Cuaderno del Instituto Vasco de Criminología*, (21), 7-32.

Del Pino, S. A. (2016). *Delitos informáticos: Generalidades*. Quito. https://repositorio.usam.ac.cr/xmlui/handle/11506/localhost/xmlui/handle/11506/2374

Donna, E. (2004). *Derecho penal: Parte especial, tomo II-B* (1.ª ed.). Rubinzal - Culzoni.

https://tsjcaba.opac.ar%2Fpergamo%2Fgeneral%2Fdocumento.php%3Fui%3D1%26recno%3D5699%26id%3DPERGAMO.1.5699

Echavarría Ramírez, R. (2022). *¿Incumplimiento contractual o delito de estafa? Criterios de delimitación en la jurisprudencia de la Corte Suprema de Justicia*. Universidad Externado de Colombia. https://bdigital.uexternado.edu.co/handle/001/13224

El capital financiero. (2024). En Panamá las estafas por medio de mensajes falsos aumentan un 224%, según estudio. *El CapitalFinanciero - Noticias Financieras de Panamá*. https://elcapitalfinanciero.com/en-panama-las-estafas-por-medio-de-mensajes-falsos-aumentan-un-224-segun-estudio/

Estrada, Y. E., & Ramos, E. L. R. (2011). El Fraude Informático. Consideraciones Generales. *Contribuciones a Las Ciencias Sociales*. https://ideas.repec.org//a/erv/coccss/y2011i2011-119.html

Faraldo Cabana, P. (2007). Los conceptos de manipulación informática y artificio semejante en el delito de estafa informática. *Eguzkilore: Cuaderno del Instituto Vasco de Criminología*, (1), 33-57.

Fernádez Teruelo, J. G. F. (2019). Respuesta penal frente a fraudes cometidos en Internet: Estafa, estafa informática y los nudos de la red. *Revista de Derecho Penal y Criminología*, (19), 217-243.

Fernández, M. B. (2004). *Los delitos de estafa en el código penal*. Editorial Universitaria Ramón Areces.

Flores, M. del C. M. (2018). Muñoz Machado, Santiago (dir.), Diccionario Panhispánico del Español Jurídico, Madrid, RAE/ Cumbre Judicial

Iberoamericana/ Consejo General del Poder Judicial-Santillana, 2017. *Revista de la Facultad de Derecho de México*, *68*(270), 927-938. https://doi.org/10.22201/fder.24488933e.2018.270.63763

FTC. (2022). Cómo reconocer y evitar las estafas de phishing. *Comisión Federal de Comercio*. https://consumidor.ftc.gov/articulos/como-reconocer-y-evitar-las-estafas-de-phishing

Galán Muñoz, A. (2003). *El fraude y la estafa mediante sistemas informáticos. Análisis del artículo 248.2 del código penal.* Universidad Pablo de Olavide. https://dialnet.unirioja.es/servlet/tesis?codigo=220244

Galán Muñoz, A. (2017). *Fundamentos y limites de la responsabilidad penal de las personas jurídicas tras la reforma de la LO 1/2015*. Tirant lo Blanch.

Gallego Soler, J. I. (2002). *Responsabilidad penal y perjuicio patrimonial*. Tirant lo Blanch. https://dialnet.unirioja.es/servlet/libro?codigo=196553

Garzón Tapia, N., & Vizuete Gallardo, M. (2009). *El fraude informático: Valoraciones técnico-jurídicas*.Universidad Técnica de Cotopaxi]. https://www.academia.edu/117188000/El_fraude_inform%C3%A1tico_valoraciones_t%C3%A9cnico_jur%C3%ADdicas

Gemma, J. (2017, octubre 23). ¿Quién es el ciberdelincuente? Del intrusismo a la maestría. *Cuadernos de Seguridad*. https://cuadernosdeseguridad.com/2017/10/infografia-quien-es-el-ciberdelincuente-del-intrusismo-a-la-maestria/

Gill, H. (2014). *Derecho penal parte general*. Juristas Panameños,.

Godoy, J. (2020). Regulaciones panameñas a los delitos informáticos que afectan los Sistemas de Información Contables Administrativos (SICA). *Orbis Cognita*, *4*(1), 113-134.

Gonzáles, M. (2014). *Fraudes en Internet y estafa Informática.*Trabajo de Grado, Universidad de Oviedo. https://digibuo.uniovi.es/dspace/handle/10651/27824

González, S. M. (2024). *Delitos informáticos en Panamá: Una amenaza que aumentó un 113% en los últimos meses*. Tvn Panamá. https://www.tvn-2.com/contenido-exclusivo/delitos-informaticos-panama-ciberseguridad-delincuentes-proyecto-de-ley-ministerio-publico-investigacion-phishing_1_2157643.html

Guerra de Villalaz, A. (2002). *Derecho penal: Parte especial*. Editorial Mizrachi & Pujol. https://books.google.co.ve/books/about/Derecho_penal.html?id=SKJ3AAAACAAJ&redir_esc=y

Guerra de Villalaz, A. (2013). Historia de la codificación penal durante la época republicana. *Órgano Judicial*. https://www.organojudicial.gob.pa/uploads/wp_repo/blogs.dir/cendoj/13-historiadelacodificacionpena.pdf

Guerra de Villalaz, A. E., Villalaz de Allen, G., & González Herrera, A. H. (2017). *Compendio de derecho penal: Parte especial* (3 ed). Portobelo. https://biblioteca.organojudicial.gob.pa/cgi-bin/koha/opac-detail.pl?biblionumber=6201

Gutiérrez Francés, M. L. G. (1990). *Fraude informático y estafa: (Aptitud del tipo de estafa en el derecho español ante las defraudaciones por medios*

informáticos). Universidad de Salamanca, Departamento de Derecho Público, Área de Derecho Penal. https://books.google.co.ve/books/about/Fraude_inform%C3%A1tico_y_estafa.html?id=dgsYnQAACAAJ&redir_esc=y

Guzmán, G., Palacios, D., & Palacios, E. (2023). Incidencias de los ciberdelitos y sus regulaciones en la ciudad de Panamá. *Semilla Científica*, (4), 524-539.

Iberley. (2024). El delito de estafa: Regulación y jurisprudencia. *Revista Juririca Colex*.

INTERPOL. (2016). *Ringleader of global network behind thousands of online scams arrested in Nigeria*. https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2016/Ringleader-of-global-network-behind-thousands-of-online-scams-arrested-in-Nigeria

Javato Martín, A. M. (2008). *Sobre Estafa convencional, estafa informática y robo en el ámbito de los medios electrónicos de pago. El uso fraudulento de tarjetas y otros instrumentos de pago*. Universidad de Granada. https://dialnet.unirioja.es/servlet/articulo?codigo=3051696

Jescheck, H.-H. (1999). *Tratadp de derecho penal. Parte general*. Comares.

Juzgado Criminal y Correccional Federal Nro. 12. (2008). *Caso Hernan Arbizu*. http://cipce.org.ar/basecausas/2201-nn-s-delito-accion-publica-jp-morgan

La Prensa. (2009). *«Phishing» causa confusión a clientes del Banco General*. https://www.prensa.com/economia/Phishing-confusion-clientes-Banco-General_0_2665233666.html

LACNIC. (2018, diciembre 19). Ciberseguridad. *LACNIC Blog*. https://blog.lacnic.net/ciberseguridad/

López, H. D. O., Alvarado, Y. R., & López, C. E. R. (2024). *Libro homenaje a Alfonso Reyes Echandía en el nonagésimo aniversario de su nacimiento*. Universidad Externado.

Machado, S. M., Española, R. A., & Judicial, C. G. del P. (2016). *Diccionario del español jurídico*. Espasa.

Martínez, G. (2025). La tormenta perfecta: El mayor ciberataque contra el sistema financiero de Brasil. *LACNIC Blog*. https://blog.lacnic.net/ciberataque-sistema-financiero-brasil/

Mata, R. (2001). *Delincuencia informatica y derecho penal*. Edisofer S.L.

Mayer Lux, L., & Oliver Calderón, G. (2020). El delito de fraude informático: Concepto y delimitación. *Revista chilena de derecho y tecnología*, *9*(1), 151-184.

Meini Méndez, I. F. M. (2012). *Teoría jurídica del delito en el sistema penal acusatorio panameño: Adaptado al Código Penal de la República de Panamá (Ley 14 de 2007), con las modificaciones y adiciones introducidas por la Ley 26 de 2008, la Ley 5 de 2009 y la Ley 14 de 2010, y al tenor de las disposiciones contenidas en el Código Procesal Penal (Ley 63 de 2008)*. Alianza Ciudadana Pro Justicia.

Miró Llinares, F. (2011). La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen. *Revista electrónica de ciencia penal y criminología*, (13), 7.

Molina Estupiñán, B. N. (2025). *Gestión y técnicas en la manipulación de datos para el área de seguridad de la información: Una revisión sistemática* [Trabajo de Grado, Universidad Politécnica Salesiana]. http://dspace.ups.edu.ec/handle/123456789/29946

Montalvo, C. (2001). Fraude informático y estafa por computación. *Cuadernos de derecho judicial*, (10), 305-352.

Mosquete, D. (1958). Antón Oneca, José: Las estafas y otros engaños, en el Código penal y en la Jurisprudencia. A*nuario de Derecho Penal y Ciencias Penales*, (2/1958), 355-357.

Muñoz, A. S. (2008). El Concepto de patrimonio y su contenido en el delito de Estafa. *Revista Chilena de Derecho*, *35*(2), 261-292.

Muñoz Conde, F. (2015). *Derecho penal: Parte especial*. Tirant lo Blanch. https://dialnet.unirioja.es/servlet/libro?codigo=614971

Muñoz Pope, C. E. (2000). *Introducción al derecho penal* (1 ed). Panamá Viejo.

Naciones Unidas. (2015). *Código Penal y Legislación Complementaria, Articulo 248*. : https://www.unodc.org/cld/en/legislation/esp/codigo_penal_y_legislacion_complementaria/titulo_xiii/article_248/article_248.html

Novoa Polanco, L. E., & Carcamo Iraheta, M. A. (2025). *Las modalidades del delito de estafa por medios informáticos como consecuencia de la evolución del comercio electrónico desde la pandemia de Covid-19* [Trabajo de Grado, Universidad de el Salvador]. https://hdl.handle.net/20.500.14492/33173

Oneca, J. A. (1957). *Las estafas y otros engaños en el Código Penal y en la jurisprudencia*. Editorial Francisco Seix.

ONU. (2018). *Cybercrime Module 2 Key Issues: Computer-related offences*. : https://www.unodc.org/cld/es/education/tertiary/cybercrime/module-2/key-issues/computer-related-offences.html

Pabón Parra, P. A. (Ed.). (2016). *Código penal de la República de Panamá: Segundo texto único y leyes modificatorias,esquemático*. Doctrina y ley.

https://biblioteca.organojudicial.gob.pa/cgi-bin/koha/opac-detail.pl?biblionumber=5922

Penal, 13° Congreso sobre Prevención del Delito y Justicia. (2015). *13º Congreso sobre Prevención del Delito y Justicia Penal, Doha, del 12 al 19 de abril de 2015*. https://www.un.org/es/events/crimecongress2015/about.shtml

Peñalba Ríos, L. G. P. (2025). La Teoría del delito en el Procedimiento Penal panameño. *Cuadernos Nacionales*, (36), 118-133. https://doi.org/10.48204/j.cnacionales.n36.a6831

Pérez, C. (2025). *¿Es necesario un cambio en la regulación debido a las nuevas tecnologías?* Trabajo de Grado, Universidad de Valladolid. https://uvadoc.uva.es/bitstream/handle/10324/79746/TFG-D_02074.pdf?sequence=1&isAllowed=y

Pérez Manzano, M. (1995). Acerca de la imputación objetiva de la estafa (1). *Hacia un derecho penal económico europeo. Jornadas en honor del profesor Klaus Tiedemann: Universidad Autónoma de Madrid, 14-17 de octubre de 1992]*. https://dialnet.unirioja.es/servlet/articulo?codigo=2071180

Plascencia Villanueva, R. (2004). Teoría del delito, 3a. Reimp. En *Https://biblio.juridicas.unam.mx/bjv/id/44*. Universidad Nacional Autónoma de México. Instituto de Investigaciones Jurídicas. http://ru.juridicas.unam.mx:80/xmlui/handle/123456789/9020

Polanio, M. (2017). *Estafa informática del artículo 248.2 del código penal* [Tesis de Doctorado, Universidad de Sevilla]. https://idus.us.es/server/api/core/bitstreams/885069f5-7725-4bd9-858f-3320feb75da1/content

Puig, S. M. (2015). *Derecho penal: Parte general*. Editorial Reppertor.

RAE. (s. f.). *Patrimonio | Diccionario de la lengua española*. Diccionario de la lengua española- Edición del Tricentenario. Recuperado 19 de abril de 2026, de https://dle.rae.es/patrimonio

Rendón, A. D. Z., Talledo, Y. K. M., Mendoza, C. M. V., & Zambrano, A. R. R. (2024). Ciberataques en América Latina: Desafíos de la era digital. *Revista Compromiso Social*, 89-104. https://doi.org/10.5377/recoso.v1i13.19295

Rodrígues de Oliveira, V. (2025). *Hacia una legitimación dogmática en el derecho penal* [Tesis de Doctorado, Universidad de Valladolid]. https://uvadoc.uva.es/bitstream/handle/10324/77776/TESIS-2515-250916.pdf?sequence=1&isAllowed=y

Rodríguez, F. (2009). *Nuevos delitos informáticos: Phising, pharming, hacking y cracking*. https://web.icam.es/bucket/Faustino%20Gud%C3%ADn%20-%20Nuevos%20delitos%20inform%C3%A1ticos.pdf

Romero Soto, L. E. (1990). *El delito de estafa* (1 ed). Carvajal. https://biblioteca.organojudicial.gob.pa/cgi-bin/koha/opac-detail.pl?biblionumber=484&shelfbrowse_itemnumber=1312

Rosso, M. (2022). *Delito de estafa informática—LegalToday*. Legal Today. https://www.legaltoday.com/practica-juridica/derecho-penal/penal/delito-de-estafa-informatica-2022-04-29/

Rovira del Canto, E. (2002). *Delincuencia informática y fraudes informáticos*. Comares. https://dialnet.unirioja.es/servlet/libro?codigo=78744

Roxin, C., Peña, D. M. L., Conlledo, M. D. y G., & Remesal, J. de V. (2003). *Derecho Penal. Parte General. Tomo I, Fundamentos. La estructura de la teoría del delito*. Civitas. https://dialnet.unirioja.es/servlet/libro?codigo=298906

Ruiz, L. C. (2006). *Delitos contra el Patrimonio. Aspectos penales y criminológicos: Especial referencia a Badajoz*. Vision Libros.

Sala de Casación Penal. (2009). *Caso nº 560 de la Corte Suprema—Sala de Casación Penal del miércoles 11 de noviembre de 2009*. vLex. https://vlexvenezuela.com/vid/elio-oswaldo-rodr-guez-n-283287067

Sánchez, A. S. (2006). La estafa informática. *Derecho Penal y Criminología*, *27*(81), 195-223.

Sánchez Bernal, J. (2009). El bien jurídico protegido en el delito de estafa informática. *Cuadernos del Tomás*, (1), 105-121.

Sanchez, J. (2000). *STS 751-2000, 3 de Mayo de 2000*. vLex. https://vlex.es/vid/fuerza-atenuante-adiccion-drogas-21-849-15199265

Sánchez Salazar, P. M., Araujo Arízaga, A. A., Salinas Herrera, F. M., Sánchez (2025). Responsabilidad penal por manipulación digital con fines delictivos: Una mirada desde el derecho digital comparado en América Latina. *Cuestiones Políticas*, *43*(83), 42-55. https://doi.org/10.5281/zenodo.17756519

Sentencia Civil de Corte Suprema de Justicia (Panama), 1ª de lo Civil, 21 de Agosto (2014). https://vlex.com.pa/vid/casacion-corte-suprema-justicia-650677041

Sentencia Penal de Corte Suprema de Justicia (Panama). (2022). *Sentencia Penal de Corte Suprema de Justicia (Panama), Sala Segunda de lo Penal, N° 290-2021*. vLex. https://vlex.com.pa/vid/sentencia-penal-corte-suprema-935105619

Sentencia Pleno de Corte Suprema de Justicia (Panama), Pleno, 2 de Julio (2014). https://vlex.com.pa/vid/impedimento-corte-suprema-justicia-592794550

STS, 21 de octubre del 1998 (1998). https://vlex.es/vid/52346266

STS, 30 de Enero del 2001 (2001). https://vlex.es/vid/revision-sentencia-penal-1995-15205876

Suárez Sánchez, A. S. (2007). Manipulaciones de tarjetas magnéticas en el Derecho penal colombiano. *Derecho Penal y Criminología*, *28*(84), 119-136.

Superior Tribunal de Justicia de Córdoba. (2014). *Recurso de casación. Nulidad. Nulidad absoluta. Efecto corrector. Afectación de garantía constitucional. Prueba indiciaria. Valoración integrada* | *Revista Pensamiento Penal*. Pensamiento Penal. https://www.pensamientopenal.com.ar/fallos/38494-recurso-casacion-nulidad-nulidad-absoluta-efecto-corrector-afectacion-garantia

Tejero, E. (2019). Dificultades jurídicas ante las conductas delictivas contra y a través de medios informáticos y electrónicos. *Revista de Pensamiento Estratégico y Seguridad CISDE*, *4*(2), 39-54.

Tenorio Pereyra, J. E. (2018). *Desafíos y oportunidades de la adhesión del Perú al Convenio de Budapest sobre la Ciberdelincuencia* ,Academia Diplomática del Perú “Javier Pérez de Cuéllar. http://repositorio.adp.edu.pe/handle/ADP/71

Terán Carrillo, W. G. (2020). La tipicidad en la teoría del delito. *Dominio de las Ciencias*, *6*(Extra 3), 141-162.

UNODC. (2018). *Análisis jurídico de los delitos contenidos en los capítulos 1, II, III y V del Título Segundo de la Ley Especial contra los Delitos Informáticos y Conexos*.

https://escuela.fgr.gob.sv/wp-content/uploads/leyes-nuevas/analisis-juridico-de-la-ley-especial-contra-los-delitos-informaticos-y-conexos-COMPLETO-CAP-I-II-III-V.pdf

Valle Matute, J. C. (2013). *El delito informático de Phishing.* Trabajo de Grado.. https://dspace.uniandes.edu.ec/handle/123456789/2819

Velásquez, F. (2014). *Manual de derecho penal: Parte general* (Ediciones Jurídicas Andrés Morales).

Veloz, V., Veloz, E., & Veloz, J. (2026). Delitos informáticos en la era digital: Retos y desafíos actuales: Cybercrimes in the digital age: current challenges and opportunities. *Revista Multidisciplinar de Estudios Generales*, *5*(1), 1-13. https://doi.org/10.70577/reg.v4i4.445

Vílchez, C. A. V., Garcia, J. M. L., Manco, D. C. L., & Quezada, N. I. C. (2025). Derechos fundamentales del justiciable VS acciones socio-jurídicas de persecución del delito. Un estado de la cuestión. *Revista Tribunal*, *5*(11), 181-197. https://doi.org/10.59659/revistatribunal.v5i11.150

Zaffaroni, E. R., Alagia, A., & Slokar, A. (2000). *Derecho penal: Parte general*. Ediar.

Zamora Acevedo, M. (2025). Delitos informáticos: La suplantación de identidad. *Revista Jurídica IUS Doctrina*, *18*(1), 15. https://doi.org/10.15517/2fm3ma36