Universidad de Costa Rica

Sistema de Estudios de Posgrado

Maestría Profesional en Ciencias Penales

La estafa informática en Costa Rica: evaluación empírica sobre su tratamiento en sede judicial.

Trabajo final de investigación aplicada sometido a la consideración de la Comisión del Programa de Estudios de Posgrado en Derecho para optar por el grado y título de

Máster en Ciencias Penales

Vivian Cubero Mora

B32186

Ciudad Universitaria Rodrigo Facio, Costa Rica

2025

"Este trabajo final de investigación aplicada fue aceptado por la Comisión del Programa de Posgrado en Derecho de la Universidad de Costa Rica, como requisito para optar al grado y título de Maestría Profesional en Ciencias Penales."

MSc. Sergio Múnera Chavarría
Director del trabajo final de investigación aplicada.

Tabla de Contenidos

Resumen

La investigación analizó el delito de estafa informática en Costa Rica desde una doble vertiente: teórica y empírica. En el plano teórico, se analizó exhaustivamente el tipo penal contenido del artículo 217 bis del Código Penal, delimitando sus elementos objetivos y subjetivos, así como las frecuentes confusiones con el delito de estafa del artículo 216 del mismo cuerpo normativo. En el plano práctico, se examinó el tratamiento judicial de la estafa informática durante las etapas preparatoria e intermedia del proceso penal, con el propósito de constatar si las causas son efectivamente investigadas por el Ministerio Público —titular de la acción penal pública— y si se configura un patrón de impunidad estructural en esta modalidad delictiva. Los hallazgos corroboran la hipótesis de trabajo: la ineficacia investigativa del órgano fiscal, aunada a la debilidad técnica del tipo penal, incide decisivamente en la impunidad de la estafa informática en el sistema judicial costarricense.

Palabras clave: Estafa informática; delitos ciberfacilitados; ciberdelitos; impunidad estructural; proceso penal. **Keywords**: cyber fraud; Cyber-enabled crimes; Cybercrime; Structural impunity; criminal procedure.

Abstract (English)

The research analyzed the crime of cyber fraud in Costa Rica from a dual perspective: theoretical and empirical. At the theoretical level, it examined in depth the criminal offense established in Article 217 bis of the Criminal Code, delimiting its objective and subjective elements, as well as the frequent confusions with the crime of fraud regulated in Article 216 of the same statute. At the empirical level, it examined the judicial treatment of cyber fraud during the preparatory and intermediate stages of the criminal process, with the purpose of determining whether cases are effectively investigated by the Public Prosecutor's Office—the body in charge of the public criminal action—and whether a pattern of structural impunity in this offense emerges. The findings corroborate the research hypothesis: the investigative ineffectiveness of the prosecutorial body, combined with the technical weakness of the offense, decisively contributes to the persistence of impunity for cyber fraud in the Costa Rican judicial system.

Introducción

La estafa informática en el derecho penal costarricense se inserta dentro de la regulación asociada a los delitos contra la propiedad (título VIII, delitos contra la propiedad, sección IV estafas y otras defraudaciones del Código Penal). Este delito se enmarca, terminológicamente, dentro del fenómeno de la ciberdelincuencia, concepto que ha sido objeto de constantes actualizaciones debido a la rapidez con la que evolucionan las tecnologías involucradas (UNODC, 2022). En Costa Rica, la tipificación específica de la estafa informática se introdujo apenas en 2012, como una respuesta legislativa a la sociedad de globalización, en la que los seres humanos, movidos cada vez más en un mundo digitalizado se ven "expuestos" al aprovechamiento ilegítimo que lesiona su patrimonio (Calderón, 2021).

Precisamente, en atención a las formas cada vez más sagaces y modernas de estafar a la sociedad costarricense, esta investigación se enmarcó en el contexto del delito de estafa informática, que aborda la manera en la que se ha desarrollado el delito y la forma en la que se investiga para sancionarlo judicialmente. Se decidió analizar la delincuencia informática—y en ello se fundamenta la **justificación de la presente investigación**— ante la sospecha preliminar de que la mayoría de las causas penales tramitadas bajo la figura de la "estafa informática" no son objeto de una investigación efectiva por parte del órgano encargado de la persecución penal (Ministerio Público). Estas causas, en lugar de concluir con un requerimiento acusatorio, suelen ser desestimadas o finalizadas mediante un sobreseimiento definitivo, sin que la investigación fiscal logre, siquiera en un grado de probabilidad, identificar a una persona individualizada como responsable de la estafa informática denunciada.

Esta situación resulta desconectada de la realidad costarricense, donde el fenómeno es alarmantemente común: Marín Castro (2022) evidenció que un tercio de los hogares del país ha sufrido estafa o intento de estafa por medios digitales desde el inicio de la pandemia. No obstante, desde la experiencia judicial de quien redacta[1], los expedientes judiciales dedicados a este delito no superan la etapa preparatoria. En la mayoría de los casos, ni siquiera se ejecutan diligencias investigativas mínimas por parte

[1] La autora, jueza penal en etapas preparatoria e intermedia, ha ejercido en veintitrés despachos judiciales, constatando que los procesos por estafa informática difícilmente superan la fase preparatoria.

del Ministerio Público, lo que sugiere la existencia de una política persecutoria implícita de inacción frente a este tipo penal.

La solicitud fiscal de archivo de estas causas penales, mediante el instituto de la desestimación o la aplicación del criterio de oportunidad parece responder, en muchos casos, a la invocación fiscal de obstáculos para determinar el elemento subjetivo del tipo penal o la insignificancia del perjuicio económico. Esta práctica no solo debilita la eficacia del sistema penal frente a la ciberdelincuencia, sino que también propicia un estado de impunidad que contrasta con la magnitud y frecuencia del fenómeno delictivo en la sociedad costarricense.

Aunado a lo anterior, en el ámbito académico, el trabajo final de investigación aplicada de Calderón Chávez (2021), se enfocó en este mismo tipo penal, abordándolo desde la óptica recursiva. En su estudio, Calderón analizó los recursos de apelación y casación penal, evidenciando la ínfima cantidad de causas penales tramitadas por ese tipo penal en las etapas posteriores al contradictorio. Dicha investigación, en conjunto con la experiencia judicial de quien redacta estas líneas, motivó la necesidad de elaborar esta investigación, que tiene como propósito explorar el origen de esa baja actividad judicial, retrotrayéndose a etapas previas (etapa preparatoria e intermedia) donde presumiblemente se encuentra el núcleo del problema identificado por Calderón Chávez.

Para ello, se trabajó con causas penales correspondientes al bloque temporal inmediatamente posterior a la investigación de Calderón (2020 a agosto 2023, inclusive) con objetivo de ofrecer al lector material actualizado, relevante y útil para fomentar la reflexión crítica desde la comunidad judicial y contribuir al mejoramiento de la administración de justicia. Ambos insumos —la evidencia empírica desde la práctica judicial y el abordaje académico previo— suscitaron una inquietud fundamental ¿existe actualmente un estado de impunidad respecto a un tipo penal cuyo auge ha sido potenciado por el desarrollo tecnológico?

Por tal motivo, esta investigación se propuso examinar si dicha percepción de impunidad responde a una realidad verificable y, en caso afirmativo, cuáles son las causas que la generan. En consecuencia, la **pregunta de investigación** que guía este trabajo es la siguiente: ¿en Costa Rica no se está investigando judicialmente el delito de estafa informática? ¿Existe impunidad en este tipo penal? Y si así fuere, ¿por qué ocurre?

En función de lo expuesto, la *hipótesis de investigación* de esta investigación razona que el delito de estafa informática no está siendo investigado efectivamente por parte del órgano fiscal, lo que estaría generando un escenario de impunidad en los delitos de estafa informática en Costa Rica. Bajo esta premisa, la investigación pretende arribar a conclusiones dominantes sobre cómo se maneja el tipo penal de estafa informática en la realidad judicial costarricense. Para los efectos indicados, el *objetivo general* que guía la presente investigación es analizar las causas penales tramitadas por el delito de estafa informática en el Primer Circuito Judicial de Alajuela a efectos determinar si el tipo penal ha sido investigado o si ha quedado impune en la práctica judicial.

Para llevar a cabo este análisis, se han definido siete **objetivos específicos** que permitirán instrumentalizar operativamente el objetivo general. En primer lugar, se propone examinar los orígenes y las motivaciones del legislador penal costarricense al momento de promulgar y reformar el tipo penal de estafa informática. En segundo término, se busca explicar los elementos objetivos y subjetivos que configuran el tipo penal de estafa informática. Posteriormente, se pretende identificar las causas penales tramitadas en el Juzgado Penal del Primer Circuito Judicial de Alajuela bajo el tipo penal de estafa informática en los años 2020 a agosto 2023.

Con base en esta identificación, el cuarto objetivo específico pretende analizar una muestra intencionada de las causas penales tramitadas por el delito de estafa informática en el Primer Circuito Judicial de Alajuela, a fin de examinar las diligencias judiciales realizadas en la etapa preparatoria e intermedia. Asimismo, el quinto objetivo específico, pretende determinar cuál ha sido el requerimiento conclusivo de la Fiscalía en la muestra analizada e identificar cuántas causas no superaron la etapa preparatoria. A partir de estos hallazgos, el sexto objetivo busca analizar los fundamentos esgrimidos por el órgano fiscal para no arribar a un requerimiento acusatorio, así como el razonamiento jurídico del Juzgado Penal de Alajuela al resolver lo peticionado por la fiscalía. Para finalmente, determinar si existe un patrón de impunidad en el juzgamiento del delito de estafa informática y, en su caso, determinar si dicho patrón es atribuible a la actuación de alguno de los operadores del sistema de justicia penal.

A efectos de operacionalizar los anteriores objetivos en variables observables y medibles, **la metodología de la presente investigación,** conforme a las categorías propuestas por Tamayo (2004), es aplicada y de tipo descriptiva. Aplicada, pues depende

de los descubrimientos y aportes teóricos, buscando confrontar la teoría con la realidad **(forma aplicada**) en tanto los descubrimientos teóricos permitirán analizar la realidad fáctica judicial; y de **tipo descriptiva,** implicará describir, registrar, analizar e interpretar -mediante técnicas de recolección de datos- la "naturaleza actual, y la composición o procesos de los fenómenos" (2004: 46). Utilizándose un muestreo intencionado de causas penales costarricenses, con el propósito final de analizar si existe impunidad en este tipo penal y, en caso afirmativo, indagar en su etiología.

Así los hechos, **la *metodología para la selección de causas penales*** se ejecutará mediante una *investigación cuantitativa*[2] *de diseño metodológico muestral intencionado*[3] (Bryman, 2012) o muestreo de conveniencia[4], que selecciona una muestra no aleatoria (Bryman, 2012 y Tamayo, 2004) de las causas penales tramitadas del 2020 a agosto de 2023 en el Juzgado Penal del Primer Circuito Judicial de Alajuela.

La elección del método de muestreo intencionado responde tanto a los antecedentes investigativos en la materia como a las **limitaciones** inherentes a una investigación de esta naturaleza. Las restricciones de tiempo, recursos y acceso efectivo a los expedientes penales en etapa preparatoria e intermedia condicionaron la posibilidad de realizar una revisión más amplia. En particular, debe considerarse que durante estas fases procesales rige el principio de privacidad de las actuaciones, conforme al artículo 295 del Código Procesal Penal. Esto implica que el acceso a tales causas se encuentra supeditado a la autorización expresa del Consejo Superior del Poder Judicial, lo que constituye una barrera logística y procedimental significativa para el desarrollo de investigaciones empíricas en esta área.

Además de lo anterior, el análisis requirió la revisión física y personal de expedientes judiciales, lo cual impuso una limitación operativa relevante. Esta labor fue realizada por una sola persona investigadora, directamente en un despacho judicial

[2] Alan Bryman en la 4ta edición de Social Research Methods explica que: "*quantitative research was outlined as a distinctive research strategy. In very broad terms, it was described as entailing the collection of numerical data, as exhibiting a view of the relationship between theory and research as deductive and a predilection for a natural science approach (and of positivism in particular), and as having an objectivist conception of social reality."*

[3] "*En el muestreo intencionado el investigador selecciona los elementos que a su juicio son representativos, lo cual exige al investigador un conocimiento previo de la población que se investiga para poder determinar cuáles son las categorías o elementos que se pueden considerar como tipo representativo del fenómeno que se estudia*." (2004: 178)

[4] "*A convenience sample is one that is simply available to the researcher by virtue of its accessibility (…) Social research is also frequently based on convenience sampling*" (2012: 201-202)

específico, lo que implicó no solo restricciones en términos de tiempo y desplazamiento de quien investiga, sino también en cuanto a la disponibilidad de espacio y tiempo del propio despacho judicial para facilitar el acceso y préstamo de los expedientes físicos. En atención a esta limitante, se procuró seleccionar un despacho judicial de alta relevancia a nivel nacional. Pues, según datos de la Dirección de Planificación del Poder Judicial[5], durante los años 2020, 2021 y 2022 se tramitaron en todo el territorio costarricense un total de 16 672 causas penales bajo el delito de estafa informática. De estas, el 46,6% (7.775 causas) se tramitaron en San José, seguido por Limón con un 16,5% (2.760 causas), Alajuela con 11,6% (1.933 causas), Puntarenas con 9,8% (1.632 causas), Cartago con 6,7% (1.120 causas), Guanacaste con 5,7% (953 causas) y Heredia con 3,0% (498 causas). Estos datos justifican la selección de un circuito con alta carga judicial en este tipo penal, al ser representativo del fenómeno que se pretende analizar.

Por lo anterior, aun cuando se desearía analizar una muestra representativa nacional de varios tribunales, se escoge el Primer Circuito Judicial de Alajuela por ser el circuito judicial que por competencia territorial analiza las estafas informáticas presuntamente ejecutadas desde los centros penales (popularmente llamados *"call centers"* penitenciarios); y por ser el tercer circuito judicial con mayor volumen de delitos de estafa informática a nivel nacional.

En atención a consideraciones ético-profesionales, se descartó la selección del Primer Circuito Judicial de la Zona Atlántica, a pesar de su alta carga procesal en la materia, debido a que quien redacta esta investigación ejerció funciones jurisdiccionales como jueza penal en todos los juzgados penales de dicho circuito, así como en el Primer y Segundo Circuito Judicial de San José durante los años 2022 y 2023. La inclusión de despachos donde la persona investigadora tuvo participación activa habría implicado el riesgo de examinar resoluciones propias o procesos en los que intervino directamente, comprometiendo así la necesaria imparcialidad en el análisis del abordaje judicial del tipo

[5] La información se extrae de la página oficial de la Dirección de Planificación del Poder Judicial, del Balance General Interactivo Para Especialistas, Detalle de Delitos, Delitos de Juzgados, donde se usaron los siguientes filtros: Filtros y segmentaciones que afectan a este objeto visual Año no es 2019 o 2023 DESC_DELITO es DELITOS INFORMÁTICOS DESC_DELITO no es (En blanco) DESC_TITULO es Estafa informática Materia es Penal; Oficina no es (En blanco) Tipo de oficina es juzgado penal, juzgado penal De Turno Extraordinario o juzgado penal Juvenil Dirección de Planificación. Poder Judicial, BALANCE GENERAL INTERACTIVO PARA ESPECIALISTAS desde la página https://planificacion.poder-judicial.go.cr/index.php/estadisticas-personas-especialistas

penal en estudio. Esta decisión metodológica responde al deber de preservar la objetividad y pureza del análisis, conforme a los principios éticos de la investigación científica en el campo jurídico.

De la mano con lo anterior, una vez iniciada la revisión empírica de los expedientes, se identificó como una limitación relevante la existencia de inconsistencias entre los datos proporcionados por la Dirección de Planificación del Poder Judicial y los expedientes efectivamente tramitados en el despacho judicial analizado. Se constató que múltiples causas físicas bajo el delito de estafa informática, localizadas directamente en el juzgado, no figuraban en la lista oficial suministrada por Planificación. Esta situación permitió concluir que el volumen real de causas tramitadas en el Primer Circuito Judicial de Alajuela fue superior al reportado en las estadísticas institucionales.

De forma paralela, también se identificó el fenómeno inverso: algunas causas contenidas en la lista oficial de Planificación no correspondían, en realidad, al delito de estafa informática, sino a figuras típicas distintas. Esta discordancia entre los datos institucionales y los expedientes judiciales generó una limitación adicional de tiempo, ya que fue necesario destinar parte del periodo originalmente previsto para el análisis sustantivo de los casos, a la verificación y depuración manual de la información. Esta situación afectó tanto la eficiencia como el alcance del trabajo empírico, al requerir un esfuerzo adicional no contemplado inicialmente

Se debe destacar que, se adoptaron medidas para garantizar el resguardo del anonimato de las personas involucradas en las causas penales revisadas, así como el tratamiento confidencial y responsable de los datos judiciales utilizados. La información extraída de los expedientes fue manejada estrictamente con fines académicos, bajo parámetros de protección de la identidad de las partes procesales, en cumplimiento con los principios de confidencialidad y reserva que rigen el acceso a la información judicial, especialmente durante las etapas no públicas del proceso penal. Estas precauciones fueron esenciales para asegurar el respeto a los derechos fundamentales, tanto de las personas investigadas como de las víctimas, así como la legitimidad ética de la presente investigación.

Ahora, en cuanto a la selección del parámetro temporal utilizado, este responde a los antecedentes investigativos del tema (que en la siguiente sección se analizan de forma más amplia), pues Calderón Chaves en su trabajo final de investigación aplicada para optar al grado y título de maestría profesional en ciencias penales (2021) analizó el tratamiento jurisprudencial de la estafa informática en Costa Rica durante los años 2014 al 2019 por parte de Sala de Casación Penal y Tribunal de Apelación de Sentencia Penal (en adelante TASP) del Primer Circuito Judicial de San José. Concluyendo que en todo ese periodo se dictaron solamente veintiún resoluciones por parte de la Sala de Casación Penal sobre este tipo penal y que, "si bien el TASP emitió mayor cantidad de resoluciones en comparación a la Sala Tercera (sic), los análisis de fondo con respecto al tipo penal fueron laxos" (Calderón 2021: 212).

Razón por la cual, este trabajo pretende analizar el origen de esta poca actividad judicial, retrotrayéndose a etapas previas del proceso penal donde podría encontrarse el núcleo del problema concluido en la investigación antes señalada. Por tanto, se decidió trabajar con un bloque temporal inmediatamente posterior al abordado por Calderón Chávez, comprendido entre los años 2020 y agosto de 2023 inclusive. Esta delimitación responde también a razones prácticas relacionadas con la cronología del proceso investigativo: esta investigación teórica dio inicio en el primer semestre del año 2023 y se extendió hasta agosto de ese mismo año; a partir de dicho mes comenzó la fase empírica, centrada en la recolección, revisión y análisis de expedientes judiciales. Esta organización metodológica permitió mantener la actualidad y pertinencia de la muestra seleccionada, así como garantizar una articulación coherente entre los antecedentes teóricos y el trabajo de campo.

Al haber expuesto los aspectos metodológicos que permiten encuadrar el marco de investigación, de seguido, se pretende analizar los **antecedentes de esta investigación**, pues se considera que, dentro de la dogmática penal costarricense la figura de la estafa informática como tal ha sido abordada de forma muy exigua. Realizado que fue en el análisis doctrinal y dogmático sobre el tema, se encontró más material nacional sobre el género (delito informático) que sobre la especie (el delito de estafa informática).

Se cuenta con algunos artículos de revista, entre los que podemos mencionar a Daniel Sánchez Hidalgo, en la Revista Judicial N°100 (LXV-53) con su artículo "La estafa. Sus elementos y problemática con los llamados delitos informáticos".

Se cuenta con el artículo redactado en 2014 por Elizabeth Guerrero y Alonso Salazar titulado "*Comentarios críticos a la reforma del Código Penal que introduce la Ley 9048 (Sobre Delitos Informáticos en el Derecho Penal Costarricense)"* que, si bien no menciona la "estafa informática" ni el artículo 217 bis, hace referencia a los elementos objetivos y subjetivos que deberían integrar la delincuencia informática (así denominado por los autores) y critica la "estafa electrónica" por no contener estos elementos.

De especial interés para la base de esta investigación, Patricia Bonilla Rodríguez redactó "El espectro actual de los delitos informáticos" publicado en la Revista Judicial del Poder Judicial en 2019, el cual no aborda el delito de estafa informática directamente, empero aborda una nomenclatura que aquí se comparte. Sea, ciberdelincuencia, y delitos «ciberfacilitados». Bonilla Rodríguez (2019) menciona el término delito informático cuando la informática sea el objeto de la acción delictiva, y no el medio para llevarlo a cabo. Menciona también que los **delitos ciberfacilitados** son aquellos delitos tradicionales que se ven amplificados o facilitados por el uso de tecnologías de la información y la comunicación (TIC). Bonilla (2019) rescata la multiplicidad de bienes jurídicos tutelados en los ciberdelitos, refiriéndose al patrimonio en delitos como la estafa y el robo cuando se ven facilitados por el uso de internet; la intimidad, el honor; la integridad sexual (en delitos como difusión de pornografía infantil, grooming y trata de personas con fines de explotación sexual pues son delitos que se ven facilitados por el anonimato y la facilidad que expone el uso de la TIC, especialmente el internet); entre otros. Por otro lado, en 2021 Luis Alonso Salazar Rodríguez publicó en la revista digital de ciencias penales N°1 (32) (13) el artículo "Sobre la "polución" del delito informático" aportando críticas a la redacción de los tipos penales.

Entre los libros nacionales existentes sobre el tema, podemos mencionar el publicado en el 2004 por Carlos Chinchilla Sandí, llamado "Delitos informáticos: Elementos básicos para identificarlos y su aplicación", en el cual, si bien para la fecha de su segunda publicación (2004) no existía el tipo penal actual "estafa informática" pues el tipo penal vigente se llamaba "fraude informático", Chinchilla lo menciona con la

denominación de “estafa”. La presente investigación retoma varios de los análisis que Chinchilla Sandí realizó en aquella ocasión.

Previo a la reforma, el autor Roberto Lemaître Picado en el año 2011 publicó el “Manual sobre delitos informáticos para la cibersociedad costarricense” el cual fue expuesto incluso en el marco de la reforma legislativa de 2012 que da origen al tipo penal de “estafa informática” propiamente. Ahora, de forma directa sobre el tema de investigación, se encuentra la obra “La Estafa Informática”, publicada en el año 2016 por Francisco Castillo González el cual sin duda es un gran insumo sobre el análisis del tipo penal que es analizado a lo largo de esta investigación. Por su parte, en su edición de 2019, Ricardo Salas Porras abordó en su libro “Derecho Penal Especial” una sección sobre el delito de estafa informática, en donde realiza un análisis del tipo penal y sus elementos.

Finalmente, en la academia costarricense estatal, existe solamente una tesis de maestría de universidades estatales sobre el tema, sea la de Freddy Calderón Chaves, "Construcción legislativa y aplicación jurisprudencial del delito de 'estafa' informática en Costa Rica del año 2014 a 2019". Donde, como bien se indicó en la metodología, se analizó el delito de estafa informática y su tratamiento judicial en la etapa de apelación (propiamente en Primer Circuito Judicial de San José) y en la Sala de Casación Penal, así como su construcción legislativa.

A pesar de los respetables antecedentes de esta investigación, persiste un amplio espectro de la estafa informática que no ha sido suficientemente explorado ni visibilizado. Así lo evidencia Castillo (2016), quien subraya la ausencia de estudios sistemáticos sobre el perfil del estafador informático en Costa Rica, así como la falta de estadísticas confiables relacionadas con este fenómeno. Esta carencia de datos fue también una de las limitaciones identificadas en la presente investigación, visibilizado incluso en lo que respecta a las ya mencionadas cifras de la Dirección de Planificación del Poder Judicial. Asimismo, se observa que, tras la reforma legislativa de 2012, el abordaje académico y técnico del delito de estafa informática ha sido limitado, lo cual contrasta con el alto nivel de sofisticación tecnológica que emplean los autores de este delito.

Sección I. Nociones Fundamentales

A continuación, se expone el análisis ejecutado al tipo penal en estudio, partiendo desde sus generalidades en la promulgación sustantiva costarricense hasta abordar los

problemas derivados de sus imprecisiones terminológicas. Se analizó el tipo penal que precedió a la estafa informática -el fraude informático-, así como sus reformas, y las diferencias sustanciales con la estafa "base" prevista en el artículo 216 del Código Penal. Este abordaje permitirá una delimitación precisa para adentrarse propiamente en el tipo penal de la estafa informática. Sea, decantar qué es una estafa informática y qué se tipificó en el artículo 217 bis. Sea, los elementos del tipo objetivo, subjetivo, sus verbos típicos, sus bienes jurídicos tutelados, las formas de aparición (consumación, tentativa, concursos), su penalidad y la forma en que la apreciación de sus elementos objetivos y subjetivos incide en el tratamiento judicial del delito apuntado. Este análisis permitirá valorar si los errores advertidos en la praxis investigativa judicial se originan en una incomprensión del tipo penal, y permitirá reflexionar sobre su tratamiento en sede judicial.

1. Generalidades y antecedentes de la regulación actual del delito de estafa informática

1.1. Generalidades: Precisiones terminológicas:

La positivización del delito de estafa informática en el ordenamiento jurídico costarricense se remonta al año 1995, con la promulgación de la Ley General de Aduanas (Salazar, 2021), la cual incorporó un capítulo sobre delitos informáticos. En su artículo 221 se incorporó sanción de prisión a quien accediere, sin autorización, a un sistema nacional informático. Haciendo referencia, en ese contexto, a los sistemas del Servicio Nacional de Aduanas.

A pesar de esta temprana incorporación legislativa, fue Chinchilla Sandí (2004) quien, desde la doctrina, formuló por primera vez la definición del término "delito informático". En términos generales, lo conceptualizó como una acción delictiva ejecutada por una persona, ya sea mediante el uso de un medio informático, o bien a través de una conducta que lesione los derechos del titular de un elemento informático, ya sea este un dispositivo físico ("hardware») o un programa ("software»).

Esta definición propuesta por Chinchilla (2004) abarca una visión amplia del delito informático, en tanto puede configurarse tanto por la utilización de un medio informático como por la afectación a este como un fin u objetivo. Sin embargo, se debe destacar que, esta conceptualización no es unánime a nivel doctrinario. Salazar (2021), por ejemplo,

aboga por la configuración del delito informático exclusivamente en función de su finalidad; afirmando que, el elemento o medio informático utilizado no debe ser el factor determinante para que una conducta ilícita se configure como un delito informático.

En un sentido similar, la Oficina de las Naciones Unidas contra la Droga y el Delito (en adelante UNODC por sus siglas en inglés) ha avanzado hacia una diferenciación más detallada de carácter taxonómico. En su informe de 2022, distingue claramente entre los delitos ciberfacilitados, la ciberdelincuencia y el delito informático. **El delito ciberfacilitado** vendría a ser cualquier delito "tradicional" que sea facilitado por el uso de tecnologías de la información y la comunicación (TIC). Por ejemplo, la estafa o la extorsión que se llevan a cabo a través de correos electrónicos o redes sociales. Y, **la ciberdelincuencia,** incluye delitos que son inherentemente tecnológicos y no podrían existir sin el uso de computadoras o redes. Así, cuando el objeto de la acción delictiva es alterar el sistema informático, UNODC ha englobado la acción delictiva dentro del término ciberdelincuencia, pues el influir en el procesamiento, ingreso, en el resultado o alterar algún sistema informático solo se puede ejecutar con uso de tecnologías de la información y la comunicación. Por lo tanto, UNODC (2022) clasifica al delito informático como una subcategoría de la ciberdelincuencia.

Esta diferenciación se resalta como fundamental, pues permite delimitar con claridad cuándo hay delito informático; esencial para determinar si podría haber entonces estafa informática, siendo el primero aquel que se comete utilizando medios informáticos y que afecta directamente a los sistemas informáticos. En ese tanto, UNODC (2022) define a la ciberdelincuencia como un término más amplio, que congloba al delito informático (delito dependiente de los medios informáticos) y a los delitos ciberfacilitados.

Ahora, en esta sección se va a estudiar la nomenclatura taxonómica del delito informático en el Código Penal costarricense, considerando que el artículo 217 bis actual describe al "ciberdelito" en forma amplia y no únicamente a la estafa informática como parte de los delitos informáticos. Sin embargo, es importante aclarar de entrada esta diferenciación de UNODC. Pues, como se puede intuir, aquella precisión terminológica no era contemplada al momento de tipificarse el delito de estafa informática en el Código Penal costarricense. En ese tanto, no fue sino hasta febrero de 2013 que, por primera vez, UNODC (2013) publicó un "Estudio integral sobre ciberdelincuencia" abordando

doctrinariamente la distinción los delitos dependientes de los medios informáticos y los delitos facilitados por los medios informáticos, lo que se alinea con la diferenciación entre ciberdelito y delito informático recién mencionada.

Se adelanta que la regulación que se ha adoptado a nivel nacional comprende tanto aquellos delitos cometidos por medios informáticos, con el uso de TIC, como los que tienen como finalidad vulnerar el *"software»* o *"hardware»* de un dispositivo, sin hacer distinción alguna. No obstante lo anterior, a efectos de comprender el artículo 217 bis en su redacción actual, se debe abordar su origen doctrinario y los motivos de su evolución al tipo penal actual.

1.2. Antecedentes del tipo penal actual. El delito de fraude informático

Como antecedente inmediato del delito de estafa informática, la ley No. 8148 del 24 de octubre de 2001, reformó el Código Penal para introducir el artículo 217 bis. La creación de este tipo penal se justificó, en la exposición de motivos del proyecto de ley, que al extraerla del Expediente Legislativo No. 14097 (2001) permite elucidar una motivación sumamente genérica y una fundamentación sobre los delitos informáticos extraída de monografías.com. En la exposición de motivos del expediente legislativo 14097 (2001) se indicó que existía una aplicación extensiva de los sistemas de información en casi todos los campos del quehacer social, y que entonces, le correspondía a la disciplina jurídica su protección y regulación, pues existía inseguridad informática. Concomitantemente, se expuso que era difícil definir lo que es un "delito informático" y, sin embargo, en aquella oportunidad, el criterio de servicios técnicos de la Asamblea Legislativa acuñó una definición de "monografías.com" como aquella que regiría nuestro Código Penal. Aquella se plasma en el expediente legislativo indicado, en la nota al pie 7 (2001), reflejando una debilidad estructural desde la construcción del tipo penal. Pues, si se revisa en su totalidad la exposición de motivos, no existió una preocupación por fundamentar las razones a partir de las cuales se consideraba que la regulación propuesta contribuía a combatir la inseguridad informática.

El artículo 217 bis, Fraude Informático, fue aprobado en 2001 con la siguiente redacción: "Se impondrá pena de prisión de uno a diez años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier

otra acción que incida en el proceso de los datos del sistema" (Código Penal, 1970, reforma del 2001, artículo 217 bis)

Desde la perspectiva del tipo objetivo, se observa que el legislador centró la conducta punible en la necesidad de influir en el procesamiento o el resultado de los datos de un sistema, omitiendo la fase de ingreso de datos. Esta omisión fue señada críticamente por Chinchilla (2004), advirtiendo que se dejaba por fuera del alcance del tipo el ingreso de datos. También se constata que tanto el fin como el medio a través el cual se comete el delito gira alrededor de la influencia que el sujeto activo tenga sobre el sistema de cómputo.

Se estableció el elemento subjetivo distinto del dolo en donde el agente procure para sí o para un tercero un beneficio patrimonial, sin requerir expresamente la producción de un perjuicio patrimonial, como sí ocurre en la estafa común. Pese a esto, tanto un sector de la doctrina como de la jurisprudencia consideraron que en realidad este artículo tipificaba una estafa informática y no un fraude informático, entendiendo que la diferencia entre ambos términos es una "relación de género a especie" (Chinchilla, 2004: 496), en la que el fraude es el concepto general y la estafa el concepto específico.

Bajo esta idea, la Sala de Casación Penal en 2009 consolidó esta línea jurisprudencial, en la que la palabra "fraude" referenciaba la realización de un *modus operandi* que caracteriza a un determinado comportamiento, encaminado, orientado y encauzado a la obtención de un beneficio patrimonial antijurídico, propio o para un tercero, utilizando para ello el error y el ardid, acciones que resultan ser, en definitiva, falsas y engañosas. De este modo, el fraude informático no representaba cualquier tipo de acción fraudulenta que surgía al utilizar un medio informático, sino únicamente cuando se refería al perjuicio económico ocasionado a consecuencia del fraude.

En consonancia con esta interpretación, la Sala de Casación Penal (2009) desarrolló una construcción dogmática según la cual existe una relación de género a especie entre el fraude informático y la estafa informática, línea que ya había sido esbozada por Chinchilla (2004). Así, bajo el análisis de sus votos, toda estafa informática sería un fraude informático, pero no todo fraude informático sería una estafa informática.

Por esta razón, dentro de la línea jurisprudencial iniciada en 2009, la Sala de Casación Penal consideró preferible, en lugar de denominar genéricamente a "fraude informático" en el artículo 217 del Código Penal, se utilizase la denominación de "estafa

informática". Tal precisión permitiría delimitar mejor el alcance del tipo, logrando diferenciarlo del fraude informático, vocablo por demás amplio que incluye una diversidad de conductas como lo sería la propia estafa, el sabotaje, los daños y el hurto informático -figura última que no se encontraba tipificada en nuestro ordenamiento-. Así, la Sala afirmó que dicho catálogo de conductas "no se podía puede considerar *numerus clausus* sino *apertus*, atendiendo a las nuevas modalidades para perpetrar delitos informáticos" (Sala de Casación Penal, voto 1055- 2009).

1.3. La reforma al artículo 217 bis y la regulación actual de la estafa informática.

A partir de las críticas a la figura del fraude informático, surgió el proyecto legislativo que culminó con la promulgación de la Ley No. 9048, Ley de Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal, aprobada el 7 de julio de 2012. En la exposición de motivos del proyecto de Ley, tramitado bajo el expediente legislativo No. 17613, "Reforma al artículo 229 bis del Código Penal y adición de un nuevo capítulo denominado 'delitos informáticos"(2009), se estableció: "En la última década, el tema de seguridad ciudadana ha empezado a tomar especial relevancia en la sociedad costarricense, al punto de ser tema de discusión al mismo nivel que la educación y la salud pública. El motivo de esta situación, no solo lo es el aumento desmedido de la delincuencia, sino la sofisticación de los métodos que aplican los antisociales para perjudicar tanto la integridad física y moral así como el patrimonio de los ciudadanos. (…) Un ejemplo de la sofisticación de estos métodos, es el aumento de los llamados delitos informáticos; según indicó el Organismo de Investigación Judicial por medio de un comunicado de prensa, al 4 de mayo de 2009 aproximadamente 25 personas habían sido estafadas por medio de delitos informáticos a través de las campañas publicitarias de los bancos estatales, en donde las víctimas revelaban sus cuentas por internet" (2009: 3).

Esta exposición de motivos en el proyecto de ley no aportó evidencia empírica suficiente, como datos estadísticos o criminológicos que justificasen la modificación del tipo penal. Se señaló que durante los primeros cinco meses de 2009 al menos 25 personas habían sido estafadas por medios informáticos, sin especificar si tal cifra representaba un incremento con respecto a años anteriores, ni cómo la formulación propuesta en la reforma contribuiría a reducir el supuesto incremento. Además, la definición de "delito

informático" que se incluyó en el proyecto fue tomada del sitio web Wikipedia, y el contexto que justificaba la urgencia de su aprobación se apoyó en una nota periodística del diario *La Prensa Libre.* Estos elementos evidencian, como lo apunta Calderón "una preponderancia de criterios y justificaciones alarmistas y populistas, con poco sustento desde el análisis criminológico y político criminal" (2021: 118).

Debe destacarse que, originalmente, el proyecto contemplaba una única pena de prisión de tres a doce años para todas las conductas que se enmarcaran en la descripción típica. Empero, en el trámite legislativo, se introdujo dos rangos de pena. Así, el artículo vigente estipula: "Se impondrá prisión de tres a seis años a quien, en perjuicio de una persona física o jurídica, manipule o influya en el ingreso, en el procesamiento o en el resultado de los datos de un sistema automatizado de información, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos, programación, valiéndose de alguna operación informática o artificio tecnológico, o bien, 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 o indebido para sí o para otro. La pena será de cinco a diez años de prisión, si las conductas son cometidas contra sistemas de información públicos, sistemas de información bancarios y de entidades financieras, o cuando el autor es un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos" (Código Penal, 1970, 217 bis).

La **distinción de dos rangos de penalidades** —de tres a seis años de prisión en la figura básica, y de cinco a diez años de prisión en la figura agravada— fue criticada por Chinchilla (2013), para quien la figura básica imputó una pena que va de los tres a seis años de prisión, (el nuevo mínimo es superior -lo cual consideró positivo-), pero redujo el extremo de diez años a únicamente seis años de prisión, "sin tomar en cuenta el grado del perjuicio patrimonial provocado con tan grave acción ilícita" (2013: 502).

Se discrepa de esta crítica. No solo porque la pena mínima de la figura básica aprobada es significativamente más elevada que la de la estafa menor (sin establecer, como sí lo hace el numeral 216, un criterio diferenciador a partir del monto del perjuicio patrimonial), sino que el establecimiento de una pena de hasta diez años de prisión en la

modalidad agravada supera cualquier pretensión punitiva, nuevamente, sin que se haya utilizado como parámetro el perjuicio patrimonial.

Al contrario de la crítica que apunta Chinchilla (2013), se considera que la pena del artículo 217 bis sí es una pena considerable, pues en su modalidad agravada necesita simplemente que sea cometida la acción contra sistemas de información bancarios para impedir incluso la aplicación de medidas alternas o el otorgamiento de un beneficio de ejecución condicional.

Más allá de esta distinción en el *quantum* de la pena, resultan evidentes las diferencias entre la regulación previa y la actual. Aunque el análisis técnico del tipo penal será objeto del próximo apartado; cabe señalar que, a diferencia del antiguo tipo penal de fraude informático, en el actual se establece no solo el verbo influir, sino también "manipular", incorporándose también como conducta penal relevante aquella que lleve al ingreso de datos.

Bien lo apuntó el Tribunal de Apelación de Sentencia Penal del Segundo Circuito Judicial de San José en el Voto No. 0738 de las 09:05 horas del 22 de mayo de 2015: "La estafa informática, amplió su configuración típica, al incluir acciones que no estaban en aquel otro delito, porque integró la acción de "manipular o influir en el ingreso" pero mantuvo el "influir en el procesamiento o en el resultado de los datos". Asimismo, para los casos en que se trate de sistemas de información bancaria, como es este asunto, elevó la pena mínima, a cinco años de prisión, (párrafo segundo del artículo 217 bis del Código Penal), en lugar del año que tenía como extremo menor, el derogado fraude informático".

Analizadas que fuesen las motivaciones del legislador para promulgar el tipo penal de estafa informática, así como su tipo penal predecesor, se considera necesario analizar el tipo penal de estafa informática en comparación con el tipo penal de la estafa "común" (artículo 216 del Código Penal), pues no solo son usualmente confundidos, sino, de su simple nominación, pareciese que uno es modalidad del otro, sin embargo, no comparten casi elementos en común, como veremos a continuación.

2. Diferencias de la estafa informática con la estafa "común" (artículo 216 v 217 bis del Código Penal)

Además de analizar el origen legislativo, para entender el tipo penal de estafa informática, se estima necesario examinar qué entiende nuestro ordenamiento jurídico, doctrina y jurisprudencia por estafa informática, y si tiene o no relación con su modalidad

"básica". Si se analiza secuencialmente el Código Penal, es factible considerar que la figura de la estafa informática (artículo 217 bis) debería tener algún tipo de relación con la estafa básica (artículo 216). No sólo por un asunto meramente semántico, pues ambos tipos penales fueron denominados "estafas", sino, además, porque se ubican dentro del Título VII. Delitos contra la propiedad, Sección IV Estafas y otras defraudaciones, lo cual permitiría presumir que por lógica y de acuerdo con la armonía de nuestro ordenamiento jurídico, tengan algunas similitudes entre sí. Los tipos penales en su versión vigente versan:

Estafa. Artículo 216.- Quien induciendo a error a otra persona o manteniéndola en él, por medio de la simulación de hechos falsos o por medio de la deformación o el ocultamiento de hechos verdaderos, utilizándolos para obtener un beneficio patrimonial antijurídico para sí o para un tercero, lesione el patrimonio ajeno, será sancionado en la siguiente forma. 1.- Con prisión de dos meses a tres años, si el monto de lo defraudado no excediere de diez veces el salario base(*). 2.-Con prisión de seis meses a diez años, si el monto de lo defraudado excediere de diez veces el salario base. Las penas precedentes se elevarán en un tercio cuando los hechos señalados los realice quien sea apoderado o administrador de una empresa que obtenga, total o parcialmente, sus recursos del ahorro del público, o por quien, personalmente o por medio de una entidad inscrita o no inscrita, de cualquier naturaleza, haya obtenido sus recursos, total o parcialmente del ahorro del público.

Artículo 217 bis.- Estafa informática Se impondrá prisión de tres a seis años a quien, en perjuicio de una persona física o jurídica, manipule o influya en el ingreso, en el procesamiento o en el resultado de los datos de un sistema automatizado de información, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos, programación, valiéndose de alguna operación informática o artificio tecnológico, o bien, 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 o indebido para sí o para otro. La pena será de cinco a diez años de prisión, si las conductas son cometidas contra sistemas de información públicos, sistemas de información bancarios y de entidades financieras, o cuando el autor es un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.

Si se analiza el tipo penal según la lectura simple y su interpretación literal – gramatical (están expresamente prohibidas las analógicas, con sus excepciones de beneficio al imputado, artículo 2 de nuestro Código Procesal y sustantivo), tenemos que el Diccionario de la Real Academia Española (DRAE de ahora en adelante) (consultado en línea el 17 de mayo de 2022), define el verbo infinitivo "estafar" como: "2. Der. Cometer alguno de los delitos que se caracterizan por el lucro como fin y el engaño o abuso de confianza como medio". De la misma manera, "estafa" refiere según el DRAE en su acepción de derecho a: "2. f. Der. Delito consistente en provocar un perjuicio patrimonial a alguien mediante engaño y con ánimo de lucro".

Ahora bien, producto de la restricción ateniente al principio de tipicidad y legalidad penal, para configurarse una estafa "básica" según lo instruido por el profesor y exjuez de la República, Manuel Rojas Salas, en su curso de derecho penal especial en la maestría de ciencias penales (2022), el artículo 216 del Código Penal Costarricense instruye una dinámica comisiva que implica (1) una simulación de hechos falsos, deformación u ocultamiento de hechos verdaderos, (2) un error o engaño como falsa representación de la realidad en una persona física, que finalmente lleve a (3) un acto dispositivo patrimonial autolesivo.

Así, el engaño en la estafa del artículo 216 del Código Penal, se configura como el "elemento esencial de la estafa para generar que el ofendido entregue la cosa, el derecho o el bien al estafador" (Castillo, 2013: 40). Lo anterior es útil para delimitar que la única forma de estafar a una persona en sentido jurídico penal es recurriendo un engaño, de tal manera que se induzca a una persona a error, para que tome una disposición patrimonial en su perjuicio o en perjuicio de un tercero. Bien lo indicaron Edgardo Alberto Donna, y Javier Esteban De la Fuente "si no hay ardid o engaño, aunque exista error y disposición patrimonial perjudicial, debe descartarse categóricamente el delito de estafa" (2004: 49). Esto es sumamente importante, pues los elementos objetivos de la estafa "común" no coinciden con los de la estafa informática, y no es admisible confundir los tipos penales entre sí.

Francisco Castillo deja muy claro en su libro (2016) la primera diferencia con la estafa informática, en referencia a la Teoría de Hart, precisamente la necesidad de un engaño. La estafa "común" o "base" requiere como elemento constitutivo un engaño, la inducción a error o el mantenimiento en éste a raíz del engaño. Ahora bien, en la estafa informática no existe ni un engaño ni una víctima de un engaño en sus elementos objetivos. De modo que suponer un error o engaño es una ficción y con ello se llega a una analogía prohibida en perjuicio de la persona imputada, prohibido por nuestra legislación. Esta es la primera de las diferencias entre los tipos penales, sin embargo, sus elementos típicos son tan disimiles entre sí que no resulta

jurídicamente correcto equipararles para considerarlos tipos penales similares, ello a pesar de que ambas acciones son denominadas “estafas”.

Sin dejar de lado que en la siguiente sección se analizará cada elemento constitutivo del tipo de estafa informática, otra de las diferencias entre los tipos penales es la necesidad de la estafa “base” de un beneficio patrimonial antijurídico para si o para un tercero; la estafa informática por su lado admite un beneficio patrimonial o (-o disyuntiva-) antijurídico, lo cual, como se verá en el análisis del tipo penal, abre el tipo a elementos no necesariamente económicos. Lo cual. a su vez, permitiría criticar su ubicación en el Título VII del Código: “Delitos contra la propiedad” pues se argumentará cómo el bien jurídico tutelado no es única y necesariamente “la propiedad”.

Por otro lado, no podemos ignorar que los verbos típicos no son los mismos y las penas tampoco son equiparables. Véase que incluso, el tipo penal de estafa “base” (216) hace una clasificación en torno al *quantum* de lo defraudado, lo cual no ocurre en el tipo penal de “estafa informática” (217 bis). Si se analiza comparativamente la penología, el extremo mínimo de la pena es mayor para la estafa informática, lo cual permitiría asumir que quienes legislaron, consideraron más reprochable “aquella conducta del agente consistente en el uso de datos indebidos, falsos o incompletos en un sistema automatizado; que aquella en la cual el sujeto activo induce a error a otra persona mediante engaño” (2021: 66).

Se podría tomar como diferencia la relación de exclusividad que existe entre los tipos penales. Castillo González (2016) consideró que la estafa informática se encuentra en una relación de exclusividad con respecto a la estafa general pues, la estafa informática tiene el papel de ser subsidiaria de la estafa común, siendo un tipo penal creado para capturar los casos que no se pueden subsumir en el artículo 216 del Código Penal. Por lo tanto, “la estafa general excluye a la estafa informática en aquellas situaciones fácticas que puedan subsumirse en ambos tipos penales” (2016: 135). Es decir, no son tipos penales armónicos ni podemos tener ambos tipos penales, es uno u otro.

Adicional a todas las anteriores diferencias, el perjuicio sufrido y la forma de comisión es diferente en cada tipo: para poder diferenciar entre uno y otro tipo penal, y clasificar correctamente la conducta típica, es necesario determinar si la disminución patrimonial fue una consecuencia inmediata de una actuación errónea de una persona (estafa base o general) o, si, por el contrario, dicha disminución patrimonial o de otro tipo es producto inmediato del funcionamiento de un sistema de procesamiento de datos (estafa informática) (Calderón 2021).

Y, como el tipo penal de estafa “común” es autolesivo, se erige como otra diferencia entre los tipos penales “quién” ejecutó la acción: la estafa “común” (216) es un tipo autolesivo,

o sea, que la persona ofendida se auto genera ese menoscabo patrimonial porque la engañaron o la indujeron a error. En la estafa informática no sucede así, el sujeto activo (no la persona ofendida) es el que ejecuta actos que le generan a otro el daño patrimonial o de otro tipo. La consecuencia de lo anterior podría generar confusiones en su aplicación práctica al intentar equiparar los elementos del tipo base (216) al informático (217 bis), lo cual sin duda sucede en la práctica judicial cuando se fundamenta que en una estafa informática se indujo a error o engañó a la víctima.

En virtud de las no pocas diferencias recién indicadas, atendiendo nuestra legislación, es criterio de quien redacta estas líneas que, en el tipo penal de estafa informática existe un desfase semántico importante, pues como se ha indicado, se denominó el tipo penal 217 bis como una estafa considerándosele "evolucionada" o "recargada" (Calderón, 2021) ya que, atendiendo a las circunstancias del tiempo presente, se le agregó el calificativo de ser "informática". Todo ello, a pesar de que los elementos objetivos del tipo no describen una acción de esa naturaleza.

Así los hechos, se debe diferir de Chinchilla Sandí, en "Delitos informáticos: Elementos básicos para identificarlos y su aplicación" (quien por un lado indicó que el nombre del tipo penal no es tan esencial, pero por otro lado expresó que el "nombre tiene la capacidad de dar mayor seguridad jurídica" (Chinchilla, 2004: 104). Pues, denominar al tipo penal "estafa informática" no generó mayor precisión y seguridad jurídica. Quien redacta estas líneas discrepa totalmente, el nombre otorgado a los delitos sí es importante y debe armonizar su nombre con su contenido. Además, se coincide con Castillo, en tanto el nombre del tipo penal ayuda a delimitar el tema y "da una mejor comprensión no sólo a los operadores del derecho, sino al público en general" (2016: 134).

Se recalca lo anterior pues, aunque parezca un mero aspecto nominal e inofensivo, tratándose de derecho penal, lo dijo bien Calderón Chávez (2021): sí resulta trascendente para todas aquellas personas procesadas por la comisión de dicha delincuencia. Pues si se considera la ansiada armonía del ordenamiento jurídico, al denominar el artículo 217 bis del Código Penal como "estafa informática", se le está considerando como una verdadera "estafa", e incluso más gravosa a criterio de quienes legislaron, fijándosele una pena de prisión desde esa perspectiva, lo cual, termina siendo contraproducente en la dosificación penal.

En virtud de haberse expuesto algunos elementos objetivos y subjetivos del tipo penal de estafa informática, así como de la penalidad y el reproche en el tipo, para diferenciarla de la estafa básica del 216, y determinar que no existe paralelismo ni similitud entre estos tipos penales, corresponde ahora explicar en detalle cada uno de los elementos objetivos y subjetivos del tipo penal estafa informática, según el artículo 217 bis del Código Penal.

3. El tipo objetivo de la estafa informática

Como se indicó en el apartado de comparación con el tipo penal de estafa "general" o "base", el artículo 217 bis del Código Penal Costarricense vigente describe el tipo penal de estafa informática, el cual versa:

> Artículo 217 bis del Código Penal. Estafa informática: Se impondrá prisión de tres a seis años a quien, (1) en perjuicio de una persona física o jurídica, (2) manipule o influya en el (4) ingreso, en el procesamiento o en el resultado de los datos de un sistema automatizado de información, ya sea (5) mediante el uso de datos falsos o incompletos, (6) el uso indebido de datos, programación, (7) valiéndose de alguna operación informática o artificio tecnológico, o bien, por (8) cualquier otra acción que (9) incida en el procesamiento de los datos del sistema o (10) que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un (11) beneficio patrimonial o (12) indebido para sí o para otro. (Código Penal, 1970, 217 bis)

La pena será de cinco a diez años de prisión, si las conductas son (13) cometidas contra sistemas de información públicos, sistemas de información bancarios y de entidades financieras, o (13) cuando el autor es un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que (14) en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos." (Los números en paréntesis no corresponden al original)

A continuación, se analizará la conducta delictiva desde sus sujetos, elementos objetivos, subjetivos, modalidades de comisión, verbos, bienes jurídicos tutelados, penalidades. Se iniciará en esta sección con los elementos objetivos del tipo penal, iniciando con el sujeto activo: "a quien".

3.1. Sujeto activo

La acción puede ser realizada por cualquier persona, es decir, el tipo penal de estafa informática es un **delito común**, al indicar *"se impondrá prisión de (…) a quien (…)"*. El tipo no requiere un autor especializado del delito (Castillo, 2016: 71). Puede ser cualquier persona física en su "modalidad simple":

Sin embargo, Calderón (2021) considera el segundo párrafo del tipo penal como un "**delito especial impropio**", ya que en el segundo párrafo estableció una agravante debido a las condiciones del autor, propiamente en los casos en que, la acción la lleven a cabo los empleados encargados de administrar o de dar soporte a los sistemas de computación. Se considera que ambas posiciones son correctas y no se excluyen entre sí.

3.2. Objeto material de la acción

El sistema automatizado de datos. El legislador indica en el artículo 217 bis, que, el agente, en perjuicio de otro, debe manipular o influir en el ingreso, en el procesamiento o en el resultado de los datos de un sistema automatizado de información. Luego indica que, se castiga a quien realice cualquier otra acción que incida en el procesamiento de los datos del sistema.

El punto central del artículo 217 bis es la noción de un sistema automatizado de datos. Así, el Convenio sobre la Ciberdelincuencia, Budapest (2001), indica en el artículo 1, inciso b) que "por datos informáticos" "se entenderá cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa destinado a hacer que un sistema informático ejecute una función.

Doctrinalmente, al referir al concepto de datos, se ha establecido que: "Datos son, al lado de "informaciones", "programas" y "procesamiento de datos", el objeto material de la acción del artículo 217 bis Código Penal, así como el concepto de "hechos" son el objeto material de la acción en el artículo 216 Código Penal […] Por "datos" debe entenderse una palabra, una imagen, un número o sonido convertido en una serie de "bit" o sea digitalizado […] La codificación de la información es un elemento constitutivo del concepto de datos. No hay ninguna restricción respecto a determinada clase de codificación. Por ejemplo, en la codificación digital que se realiza por medio del código binario pueden codificarse expresiones escritas y expresiones orales y otras características de un ser humano. Lo que guarda el inicio del proceso puede ser una expresión escrita ("password"), puede ser una palabra de determinada persona (proceso que se inicia con la voz de una persona) o puede ser una característica individual (por ejemplo, la huella digital, el color del iris de los ojos de una persona)" (Castillo, 2016: 36)

Así, el tipo penal de estafa informática integra una limitación del posible contenido de los datos, reflejado en los siguientes adjetivos: "uso de datos falsos o incompletos", "uso indebido de datos", y el requisito de que el autor del delito produzca con la manipulación de datos un daño patrimonial" (Calderón 2021: 86) o indebido. Sobre este último aspecto, la necesidad de que el uso de datos falsos o incompletos o el uso indebido de datos genere efectivamente un resultado lesivo patrimonial no hay un único criterio, porque, como se verá más adelante, un sector de la doctrina (Castillo, 2016) analiza la posibilidad de la lesión en abstracto sin perjuicio patrimonial. Se ahondará en las formas de aparición del delito.

Sobre el objeto material, Castillo mantiene que la utilización de un programa falso encaja perfectamente en el tipo penal, toda vez que un programa se compone datos, por lo que es falso un programa cuando las "órdenes de trabajo establecidas por medio de datos llevan a un

resultado que objetivamente se apartan del resultado a que se llegaría si no hubiera habido la manipulación del sistema de procesamiento de datos" (2016: 93).

3.3. Verbos típicos y modalidades de la acción punible. Tipo penal abierto.

El tipo penal refiere: "(…) manipule o influya en el ingreso, en el procesamiento o en el resultado de los datos de un sistema automatizado de información, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos, programación, valiéndose de alguna operación informática o artificio tecnológico, o bien, por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta (…)".

A. Uso de datos falsos, incompletos, indebidos o de programación. Valerse de operación informática o artificio tecnológico. La primera conducta que describe el artículo 217 bis para configurar el tipo penal de estafa informática es el verbo "usar", usar datos falsos, usar datos incompletos, usar datos indebidos o de programación, "valiéndose" de una operación informática.

Una vez realizado alguno de esos comportamientos humanos, necesariamente para subsumir la conducta en el tipo penal, debe influir o incidir en el procesamiento de los datos del sistema o dar como resultado información falsa, incompleta o fraudulenta, procurando obtener un beneficio patrimonial o indebido para sí o para otro.

Entonces, el verbo típico usar nos contempla dos modalidades de la acción punible, sean el uso de datos falsos o incompletos (1) y el uso indebido de datos o de la programación (2):

La primera modalidad, refiere a la necesidad de datos falsos cuando contradicen la realidad; falsedad de los datos significa falsedad de la información codificada (Castillo, 2016: 87), no se incluye en esta primera modalidad los datos que se utilizaron sin autorización (estos serían datos verdaderos usados de forma indebida). Por su parte, los datos incompletos son una subcategoría de los falsos, toda vez que terminan siendo datos no concordantes con la realidad. Ya sea mediante los datos falsos o incompletos, el sujeto activo debe influir en el resultado del equipo de procesamiento de datos. (2016: 88)

La segunda modalidad de acción, sobre el uso indebido de datos (o de) programación, es explicada por Castillo (2016) de forma que se trata de una "influencia no autorizada por medio de datos o programas correctos, de personas no autorizadas o autorizadas para otros fines en el proceso automatizado de datos de una computadora" (2016: 88). Es decir, el uso indebido de datos o programación refiere a datos que concuerdan con la realidad. Generándose una influencia no autorizada, por medio de datos o programación correctos, de personas no

autorizadas (o autorizadas para otros fines) en el proceso automatizado de datos de una computadora.

Previo a abordar lo que Castillo ha explicado como una **tercera modalidad de acción,** sea "valerse de alguna operación informática o artificio tecnológico o bien por cualquier otra acción que incida en el procesamiento de datos del sistema o que dé como resultado de información falsa, incompleta o fraudulenta"; es menester aclarar que el artículo 217 bis incluye en su redacción los verbos "manipular", "influir" e "incidir", siendo estos dos últimos producto de las acciones descritas supra (Castillo, 2021: 57). En la doctrina no es "pacífico" si estas dos palabras (influir – incidir) son verbos típicos o resultados intermedios. Francisco Castillo, en su oportunidad difirió del criterio del Carlos Chinchilla en cuanto a los comportamientos humanos que permiten cometer la estafa informática, específicamente en cuanto a influir o incidir: "Dicho con todo el respeto para el colega Dr. Chinchilla, lo anterior, según nuestro criterio, es equivocado, pues las expresiones que definen las alternativas de acción son las siguientes: mediante el uso de datos falsos o incompletos, mediante el uso indebido de datos, de programación o bien mediante cualquiera otra acción que incida en el procesamiento de datos del sistema. De modo, entonces, que influir o incidir en el sistema automatizado de datos son resultados "intermedios" de las acciones punibles, que se dan antes de producir el resultado final, que es la transferencia de un valor económico del patrimonio del perjudicado al patrimonio del autor o de un tercero." (2016: 80-81)

Sin embargo, se debe coincidir con Calderón (2021), en tanto lo esencial es que deben tener la capacidad de incidir o influir en el sistema. Por lo anterior, resulta necesario darles contenido a los verbos infinitivos: manipular, influir e incidir comprendidos en el 217 bis del Código Penal.

B. Manipular: consecuencia, no verbo típico. Ciertamente no existe ningún criterio diferenciador en el artículo 217 bis del Código Penal, mediante el cual se discrimine, si prevalece la manipulación en el ingreso de datos o el uso de datos indebidos, no obstante, ambas descripciones no deben confundirse. El uso de datos constituye el verbo del tipo penal, mientras tanto, la manipulación en sentido estricto es una consecuencia que debe cumplir el sujeto activo después de usar datos falsos o incompletos (Calderón, 2021). Incluso Calderón afirma que el uso indebido de datos ya contiene de por sí, una manipulación en sentido amplio.

Se comparte el criterio de Calderón Chaves, en atención a Castillo González, en tanto el verbo manipular en la redacción del tipo sale sobrando, dado que una manipulación solamente es punible en la medida en que influya en el resultado del trabajo del sistema automatizado de datos. Influencia en el procesamiento automatizado de los datos del sistema debe haber "en

todas las modalidades de acción descritas en el artículo 217 bis (uso de datos o programas falsos o incompletos, el uso indebido de programas o de datos en el procesamiento automatizado de datos)" (Castillo 2020: 292).

Finalmente, se mencionó la ingeniería social para acceder al uso de datos, pues debe tenerse en cuenta que, no es poco común que se confunda la ingeniería social como el engaño en la estafa simple. Sin embargo, debe recordarse que el **engaño no forma parte de los elementos objetivos del tipo penal de estafa informática.** La ingeniería social en la que la persona ofendida pueda haber sido inducida a error para dar datos es solo un medio de comisión (no típico) para el delito. Pues en la estafa informática (artículo 217 bis del Código Penal), la inducción a error no es un elemento objetivo del tipo, tal cual lo ha establecido el Tribunal de Apelación de Sentencia Penal del Primer Circuito Judicial de San José en resolución Nº 00349 – 2021, y como se explicó supra, ya que la conducta típica recae sobre el uso de datos indebidos.

C. Influir. A efectos de delimitar, de forma literal-gramatical el término, el Diccionario de la Real Academia Española ha definido "Influir" como: "1. Dicho de una cosa: Producir sobre otra ciertos efectos; como el hierro sobre la aguja imantada, la luz sobre la vegetación, etc..". Bajo este entendimiento, "efecto" debe entenderse definido por la RAE como "1. m. Aquello que sigue por virtud de una causa […] 3. m. Fin para que se hace algo. El efecto que se desea. Lo destinado al efecto…".

Castillo González en La estafa informática de "*Lege lata"* y de "*lege ferenda*" (2020) ha dejado claro que el verbo infinitivo "influir", es un resultado intermedio de la acción humana realizada por el sujeto activo. O sea, para que la conducta sea típica, debe *producir efectos* en el sistema informático, y, como bien lo explica Calderón (2021) ello lo alcanza el sujeto activo de la conducta mediante el uso de datos falsos, incompletos o indebidos, así como cualquier otra acción que ponga en marcha "el sistema" para obtener un resultado.

D. Incidir. El tipo penal establece: "por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta (…)"

El Tribunal de Apelación de Sentencia Penal del Primer Circuito Judicial de San José en su resolución Nº 01627 – 2013 y la Sala de Casación Penal en resoluciones como la 148-2006, 763-2006 y 208-2009 han establecido que "de acuerdo con la redacción de la norma en el Código Penal vigente, la acción del sujeto activo consistirá en influir en el procesamiento o el resultado de los datos de un sistema de cómputo, a través de varias conductas que han de incidir en el proceso de los datos del sistema". Así, influir en el procesamiento o resultado de los datos

incluirá manipular la información, alimentar el sistema de forma irregular, actos que incidirán en el proceso de los datos, es decir, en la realización de las instrucciones de un sistema.

Para Calderón (2021), **incidir es otro resultado intermedio de la acción humana en el delito de estafa informática**, según se presenta antes de que se produzca el resultado final, consistente en transferir el valor económico de la víctima hacia el patrimonio del imputado o de un tercero.

Ahora, Lemaître Picado (2011), refiere a las etapas del delito (en aquel entonces fraude informático) indicando que manipular información o alimentar el sistema son actos que desde el inicio no están influyendo en el procesamiento, pues, si por ejemplo, en la nómina de pagos de un sistema desde el inicio se modificó un dato de la nómina no se está alterando el procesamiento (la etapa de procesamiento), el equipo informático estará procesando los datos "correctos", según se introdujeron, su proceso es correcto según los datos que se le han dado, se está hablando de la etapa de entrada de datos, no del procesamiento de datos ni del resultado esto es así, porque con base en la función que realiza un sistema de cómputo se tienen cuatro componentes: entrada, procesamiento, salida y almacenamiento (2011: 121-122).

Bajo la inteligencia de Lemaître (2011) y de Calderón (2021) si el tipo penal habla de influir en el procesamiento o el resultado, pareciese que la etapa de entrada no está contemplada en el tipo (la introducción de datos), quien redacta estas líneas discrepa respetuosamente de tal afirmación. Pues, si bien no se estaría influyendo en el procesamiento, el tipo penal indica "por cualquier otra acción que incida en el procesamiento de los datos del sistema **o** que dé como resultado información falsa, incompleta o fraudulenta…" es decir, al tener una "o" disyuntiva se deja la posibilidad de comisión del hecho típico con otra acción como la introducción de datos que dé como resultado la información falsa, incompleta o fraudulenta lo cual a criterio de quien redacta, está incluido en el siguiente acápite.

E. Cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta. La última modalidad de comisión de la acción penal, "valiéndose de alguna operación informática o artificio tecnológico, o bien, por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta" es el ejercicio legislativo encaminado a tratar de prever acciones u omisiones que incidan en el resultado del procesamiento de datos del sistema, con la finalidad de obtener una ventaja patrimonial o indebida para sí o para un tercero.

La finalidad de la última modalidad de acción del artículo 217 bis del Código Penal fue, según Castillo (2016), prever futuras técnicas de manipulación informática, desconocidas hoy

día, que pudieran ponerse en ejecución. Cuando una de estas técnicas de manipulación tecnológica nueva aparece y no está prevista en las dos primeras alternativas del artículo 217 Código Penal sería subsumible en la tercera alternativa, lo cual deja entrever una técnica legislativa con roces de constitucionalidad.

En las dos primeras modalidades de comisión, el tipo penal describe conductas de manipulación o de uso sin permiso de datos específicamente determinadas, por lo cual se sabe respecto a esas hipótesis cuáles son las conductas punibles y cómo inciden sobre el sistema de procesamiento de datos. Sin embargo, **esta última modalidad de comisión violenta el principio de legalidad penal pues introduce un tipo penal abierto** que no permite saber de forma certera cuál es la conducta penal punible. Esta tercera modalidad de comisión es básicamente una previsión que realizaron las personas que legislan, vislumbrando que a futuro puedan existir nuevas técnicas de manipulación informática, sin indicar cuáles puedan ser. Lo cual, a criterio de quien redacta estas líneas, genera que esta tercera modalidad de comisión, indeterminada, lesione el artículo 39 de la Constitución Política.

Conforme al principio de legalidad penal consagrado en el numeral 39 de nuestra carta magna, es necesario que la ley penal describa de forma clara y previa la conducta punible para que las personas sepan a qué atenerse. Respetuosamente, sobre este punto se diside parcialmente del criterio de Castillo González quien considera que el texto actual de la variante tercera del artículo 217 bis Código Penal "tiene serios problemas de redacción y de concepto" (2016: 108), lo cual compartimos enteramente. Sin embargo, indica Castillo que su redacción no viola el principio de legalidad en su dimensión de principio de taxatividad porque el tipo penal creado por ese artículo es un delito de resultado, en el cual está prevista la causación del resultado, siendo que la forma y el modo de cómo describe el legislador esa causación no afecta al principio de legalidad.

Se respeta, mas no se comparte del todo este criterio, en tanto el ejercicio de legislar debe cumplir con los subprincipios de *lex certa y lex stricta*, los cuales derivan del principio de legalidad; con la estafa informática en la reforma del artículo 217 bis se creó un tipo penal abierto. Si bien se requiere un resultado, lo cierto del caso es que sí se considera necesario se indique cuál acción que produce ese resultado es o no ilegal. El grado de incerteza e indeterminación jurídica que acarrea incluir un tipo penal que no dice cuál otra acción entra en el delito no pasa los estándares mínimos de tipicidad legal establecidos por nuestra legislación, considerando quien redacta estas líneas, que esta última línea genera un tipo penal abierto y violatorio del principio de legalidad.

4. Bien jurídico tutelado: tipo penal pluriofensivo

Si bien la doctrina ha considerado a la estafa "básica" el tipo penal por antonomasia protector del patrimonio (Donna & de la Fuente, 2004), al punto de l afirmarse que el concepto de patrimonio nace por y para la estafa y se desarrolla a partir de sus exigencias (Conde-Pumpido Ferreiro, 1997), lo cierto del caso es -como ya se ha señalado- la estafa "básica" y la estafa informática difieren en sus elementos típicos.

En este sentido, aunque Castillo (2016) sostiene que el patrimonio es el único bien jurídico tutelado por el numeral 217 bis del Código Penal, de forma respetuosa no se comparte tal afirmación. Por el contrario, a partir de un análisis atento de la redacción del tipo penal, se considera que este protege varios bienes jurídicos, configurándose un tipo penal de carácter pluriofensivo.

La tutela del patrimonio es, ciertamente, evidente: el tipo penal alude expresamente a la obtención de un "beneficio patrimonial". Sin embargo, introduce también -de forma disyuntiva- la expresión "o indebido". En atención a la interpretación literal-gramatical, la redacción disyuntiva hace que baste entonces con la existencia de un beneficio indebido, no necesariamente patrimonial para que se constituya el tipo penal y se abra la posibilidad de resguardar la tutela de otros bienes jurídicos además del patrimonio.

Uno de estos bienes jurídicos es **la autodeterminación informativa**, cuya relevancia ha cobrado particular importancia en el contexto contemporáneo de protección de datos personales. En respaldo de esta postura, resulta oportuno traer a colación el criterio de Ricardo Salas (2019), quien afirmó que: "(…) por la redacción concerniente al dolo específico, hay una diferencia importante entre este y el de la estafa común. En el artículo 216 se dice que es "(…) para obtener un beneficio patrimonial antijurídico para sí o para un tercero (…)"; en tanto que en el 217 bis se dice que es para procurar u obtener "(…) un beneficio patrimonial o indebido para sí o para otro" (subrayado suplido). En otras palabras, **el beneficio buscado no siempre tiene que ser patrimonial, sino que basta con que sea indebido, lo cual abre el marco de posibilidades a todas aquellas situaciones provechosas contrarias al Ordenamiento Jurídico,** sin necesidad de que sea de índole patrimonial" (2019: 161)

Como puede observarse, a pesar de que Salas se refiere a un elemento subjetivo distinto del dolo, la cita permite el análisis de los distintos bienes jurídicos que el artículo 217 bis protege. Nótese que, en el fondo, la estafa informática, termina sancionando a quien utilice datos de forma indebida, en una de sus modalidades de comisión (Lemaître, 2020). En el mismo sentido, Calderón (2021) también ha indicado que la redacción del artículo 217 bis del Código Penal permite la posibilidad que, en aquellas formas de comisión del hecho mediante datos

falsos e incompletos, se vulnere la "integridad de los datos de un sistema". Así, cuando se hace uso de datos falsos o incompletos, se termina afectando la información del sujeto pasivo, aquella que está resguardada en instituciones financieras, por ejemplo.

Bajo esta línea de pensamiento, al utilizar los datos de una víctima sin su consentimiento (información que además de privada es valiosa, y que el sujeto activo se hizo de ella por algún medio) los derechos de privacidad e intimidad se verán lesionados, integrados ambos en el derecho ya expuesto de la autodeterminación informativa.

Por su parte, Gustavo Eduardo Aboso en el capítulo VIII "Delitos contra la propiedad (I): Estafa y fraudes informáticos" de su libro Derecho penal cibernético, señala que junto al objeto de protección "patrimonio" en el tipo penal de estudio también confluyen "otros intereses penalmente tutelados que se identifican con la integridad, el correcto funcionamiento y la facultad de disposición de datos, se solapan en muchos sentidos desde el punto de vista del objeto penalmente tutelado, al extremo de constituir "tipos penales conglomerantes" en razón de la pluralidad de intereses protegidos en juego" (2017: 299).

1. El tipo subjetivo de la estafa informática

Mediante resolución colegiada de Garay Boza, Chinchilla Calderón y Jiménez Fernández, el Tribunal de Apelación de Sentencia Penal II Circuito Judicial de San José abordó el contenido del tipo subjetivo en los delitos dolosos. Citando a Tavares Juárez (2013), el tribunal señaló que el tipo subjetivo se compone del dolo, como elemento subjetivo general y de intenciones, de tendencias o percepciones, como elementos subjetivos distintos del dolo.

En el tipo penal de estudio, la tipicidad subjetiva de la estafa informática requiere dolo directo, el cual refiere al conocimiento y voluntad de realización de los elementos específicos del tipo objetivo junto con los elementos subjetivos distintos del dolo. Es decir, el autor directo del delito de estafa informática actúa dolosamente cuando sabe que está usando datos falsos, datos incompletos, datos indebidos o de programación, "valiéndose" de una operación informática que manipula estos datos y quiere como resultado final un beneficio patrimonial o indebido para sí o para otro. Hay que recalcar que esta fórmula de conocimiento de todos los elementos subjetivos del tipo es el **arquetipo para la autoría directa**; sin perjuicio de los institutos amplificadores del tipo (coautoría, participación) sobre los cuales se ahondará infra.

Se debe indicar que, Castillo (2016) equiparara el tipo subjetivo del artículo 217 bis con el previsto para la estafa del artículo 216 del Código Penal. No se comparte esta posición pues la estafa del artículo 216 solo protege el patrimonio, mientras que la estafa informática presenta un alcance más amplio. Como se ha argumentado, el elemento subjetivo no se agota únicamente con el conocimiento de la manipulación de los datos falsos, incompletos, indebidos

o de programación, valiéndose de una operación informática, pues existen elementos subjetivos distintos del dolo, conforme se expone.

5.1. El dolo y la intención de obtener un beneficio patrimonial antijurídico o un beneficio indebido. Elementos subjetivos distintos del dolo.

Respecto del alcance del dolo, se debe reiterar la observación de Salas (2019), quien subraya una diferencia relevante en la redacción concerniente al dolo específico entre la estafa informática y el dolo de la estafa común.

En la estafa "común" del artículo 216 del Código Penal, impera el obtener un beneficio patrimonial antijurídico para sí o para un tercero, a diferencia del artículo 217 bis (estafa informática) cuya redacción incoa "*procurar u obtener* un beneficio patrimonial **o** indebido para sí o para otro". Esto se traduce en que, el beneficio buscado no siempre tiene que ser patrimonial, sino que basta con que sea indebido. Y, la redacción incluye no solo obtener el beneficio, sino también procurarlo. Esta frase, también nos permite vislumbrar los elementos subjetivos distintos del dolo que requiere el tipo penal. Es decir, los elementos intencionados requeridos por el tipo: el propósito o la intención del autor de procurarse u obtener un beneficio patrimonial o indebido para sí o para otro.

Castillo (2016) atina indicando que las manipulaciones culposas que pueden provocar un desplazamiento patrimonial de una cuenta ajena a otra propia no son punibles penalmente, aunque pueden ser civilmente relevantes. En este extremo se coincide plenamente. Sin embargo, los alcances del dolo en la autoría y participación sí han sido objeto de discusión jurisprudencial. Lo que hace necesario exponer un análisis de los elementos que debe abarcar el dolo en los casos de coautoría y participación.

5.2. Institutos amplificadores del tipo: análisis de los elementos que debe abarcar el dolo en la coautoría y participación.

Respecto de la autoría y participación, resultan aplicables las reglas generales: cualquier persona puede ser autor. En el caso de la coautoría por distribución de funciones, la experiencia judicial acumulada evidencia que la modalidad más recurrente de estafa informática[6] implica una dinámica comisiva articulada. En la que, personas usualmente desconocidas, ingresan a los sistemas bancarios de la persona ofendida y manipulan el mismo, para trasladar sus fondos hasta

[6] En la segunda parte de esta tesis se presenta un análisis empírico de las causas penales de estafa informática tramitadas en Costa Rica entre el 2020 y 2023. Para ellos se empleó un modelo de regresión lineal múltiple, que permitió identificar patrones comunes en el modus operandi de las estafas informáticas. Se sugiere revisar dicha sección y los anexos correspondientes para un mayor detalle sobre la sistematización y hallazgos obtenidos.

una cuenta específica. La persona dueña de esta cuenta, o la persona que retira el dinero de esta cuenta es quien normalmente se apunta como imputado, al haber recibido o retirado el dinero defraudado. Este personaje, es usualmente llamado en la jerga judicial "frenteador".

Este frecuente caso, será expuesto en la segunda parte de este trabajo, pues al realizar levantamientos de secretos bancarios, es posible determinar la cuenta de la persona ofendida de donde se extrae dinero y la cuenta de la persona que la recibe. En este caso particular (y máxime siendo el "más usual"), se considera absolutamente necesario analizar la existencia de coautoría por contribución determinante y esencial para la consumación del delito, o (según los elementos de cada caso en concreto) al menos, complicidad como instituto amplificador del tipo. Pues se debe recordar que los institutos amplificadores del tipo permiten imputarle actos a una persona que no ha realizado personalmente.

Ahora, si bien existe un tema de fondo casuístico que atañe a las particularidades probatorias de cada caso (ya que per se, el hecho de recibir el dinero en una cuenta y /o hacer el retiro del dinero fraudulento, no implica necesariamente que se está ante un coautor o un cómplice de estafa informática) sí se debe analizar la intervención de la persona que recibe en su cuenta bancaria el dinero conseguido mediante una estafa informática, pues desde la tipicidad subjetiva se debe analizar si concurre o no algún instituto amplificador que permita clasificarle como coautor o cómplice.

Bajo esta inteligencia, el coautor en este escenario específico tiene conocimiento del origen ilícito de los fondos, tiene conocimiento del plan previo y del rol que le corresponde en esa ejecución del plan (recibir los fondos en su cuenta, la distribución funcional); así como que existió otro sujeto encargado de la manipulación de los datos de un sistema automatizado de información o, al menos, lo acepta. Este análisis, ha sido expuesto por el Tribunal de Apelación de Sentencia Penal (en adelante TASP) del Primer Circuito Judicial de San José en la resolución 00256 - 2023 del veinte de febrero de dos mil veintitrés. En donde consolidó una línea la línea expuesta previamente en la resolución número 0512-2021, sobre el **análisis requerido del dolo específico cuando tenemos al llamado "frenteador**" en la estafa informática, que no fue directamente quien hizo (o no se puede demostrar) la transferencia bancaria fraudulenta, sino que recibió y/o retiró el dinero fraudulento.

Así, estableció el TASP en el voto de cita: "Nótese que el tipo penal requiere una acción directa del agente. Pero nunca se atribuyó (ni se demostró) que el endilgado hubiese efectuado, de propia mano, es decir, por sí mismo, esa conducta. En otras palabras, ni se acusó ni acreditó que el encartado hubiese sido quien manipulara o influyera en los datos del sistema bancario para extraer el dinero del ofendido y depositarlo en su cuenta. **Lo que se pretendió acusar fue**

que existía un plan previo entre el sujeto que así lo hizo y el imputado para tal proceder y que, en virtud de dicho plan, hubo una distribución de funciones entre ambos sujetos: uno haría el movimiento en la cuenta y extraería el dinero y otro prestaría su cuenta para que se depositara y lo recuperaría. Este mecanismo dogmático permite imputarle actos a una persona que no ha realizado personalmente. Es decir, se acusó una coautoría que, entonces, introduce varios elementos fácticos en la configuración típica: uno objetivo (la distribución funcional necesaria para la comisión) y uno subjetivo (el plan previo). Así planteado el tema, **el dolo debe abarcar también esos elementos. Es decir, el dolo en una coautoría no implica solo** (…) **que el encartado conociera el origen ilícito de los fondos sino, también, que él conociera el plan y el rol que le correspondía tanto a él como al otro sujeto en la manipulación de los datos de un sistema automatizado de información y, al menos, lo aceptara (dolo eventual). Ese conocimiento previo a los hechos es vital para distinguir la figura de la coautoría de otras como la complicidad**" En este caso concreto, la acusación otorga al encartado un papel específico, crear y facilitar la cuenta para acreditar y luego retirar los fondos, **sin que sea necesario que fuera él quien llamó a la víctima** y/o realizó la transferencia pues una vez acreditados los fondos corrió al banco a sacar el dinero. (Tribunal de Apelación de Sentencia Penal del II Circuito Judicial de San José, Resolución Nº 00256 – 2023; la negrita es del original).

Este voto es de particular importancia para el análisis del delito de estafa informática en la práctica. Pues, como se verá en la segunda parte, existe un gran sector judicial que considera que a los "frenteadores" no se les puede achacar el ilícito del 217 bis al considerar imposible determinar su participación o coautoría. No se comparte esta posición, pues **el dolo es por excelencia un instituto que se prueba de forma indiciaria** y al existir institutos amplificadores del tipo se considera que se debe aplicar un análisis que permita examinar la coautoría, complicidad o la inexistencia de estos. Como bien lo ha indicado el Tribunal de Apelación de Sentencia Penal del Segundo Circuito Judicial de San José, en la resolución 1838-2022 de las 09:15 horas del 20 de diciembre de 2022 al analizar el dolo del autor en delito de estafa informática y la responsabilidad del titular de la cuenta bancaria, así como la importancia de la prueba indiciaria recabada en la investigación:

"(…) En otro orden de reclamos, se alega que el elemento subjetivo del tipo penal no se puede inferir de la prueba y por eso no se logró sustentar en la sentencia. Lo primero que debe acotarse es que **el dolo del autor, a menos que exista una confesión, no puede acreditarse**

con prueba directa, sino que se determina de manera inductiva. De ahí la necesidad de ponderar, en cada caso concreto, la coincidencia entre la finalidad perseguida y la obtención de esta mediante acciones directamente encaminadas hacia dicho fin. Es decir, deberá verificarse la existencia de acciones que pongan en evidencia la voluntad de realizar la acción delictiva. El tribunal de juicio, haciendo ese ejercicio indicó: […] Como se puede colegir, y sin que haya sido cuestionado la acreditación de estas circunstancias y acciones del imputado por parte de la defensa, el aquí justiciable abrió la cuenta de destino un día antes de que se realizaran las transferencias fraudulentas; le ingresó a su cuenta dinero en colones que correspondía a la misma cantidad del dinero en dólares que le fue sustraído de la cuenta de la víctima; la persona ofendida no conocía al encartado ni tenía tratos comerciales con este, lo que tornaba la trasferencia de dinero carente de justificación alguna; el encartado, a pesar de conocer que ese dinero no poseía justa causa procedió a su retiro en su totalidad -a través de la ventanilla del banco y del cajero automático-; y esta acción de egresar el dinero de la cuenta se dio menos de una hora después...de que se efectuara la sustracción dineraria. Estos son indicios, claros, precisos y graves, y resultan contundentes cuando se aplica la regla de experiencia que indica que en este tipo de delitos informáticos, en donde media la obtención de información privilegiada de la víctima para influir en un sistema informático bancario, desde donde manipular una cuenta de origen y así realizar traslados de dinero a otras cuentas, los partícipes del delito siempre lo harán hacia cuentas de destino donde tengan posibilidad de disposición (ya que se trata de una actividad criminal lucrativa y no de beneficencia) y, desde donde, en un tiempo rápido, poder retirarlo o transferirlo a otras cuentas bancarias para diluir su rastro y la posibilidad de que las autoridades bancarias, ante la alerta de las víctimas, congelen estos movimientos. Precisamente, el imputado cumplió con todos estos parámetros. Nótese que, previo a los hechos el justiciable no tenía cuentas bancarias y la que abrió fue justo un día antes de que se diera la alteración del sistema informático que afecto las cuentas de la víctima, por lo que, necesariamente tuvo que conocer que a su haber llegaría una suma de dinero que se transferiría a través del sistema bancario nacional. Asimismo, transferido el dinero de la víctima, luego de influirse fraudulentamente en el sistema, el encartado no esperó mucho para, a través de la ventanilla de la institución bancaria y el sistema de cajeros automáticos, retirar el monto defraudado; lo que significa que aquel conocía que podía disponer de ese dinero y que debía hacerlo lo antes posible. Y, además, no fue cualquier monto el que retiró, sino que lo hizo en la totalidad del que le había sido transferido, lo que representaba un conocimiento de que era necesario evitar dejar algún remanente en la cuenta bancaria. Estos indicios, de manera concatenada, no permiten llegar a otra conclusión que a la descrita en sentencia, de que

el endilgado conocía de la manipulación del sistema informático que se iba a realizar para sustraer dinero y que decidió apoyar el plan de autor, para lo cual abrió una cuenta bancaria para recibir los fondos, como finalmente ocurrió, y una vez con la suma defraudada en su haber procedió a retirarlos para asegurar el botín. La defensa pública fustiga que no solo la hipótesis acusatoria podría ser válida, sino también una culposa, sin embargo, ninguno de los elementos de prueba citados o de los medios probatorios incorporados al debate muestran esa hipótesis, al menos, como posible, por el contrario, **los actos que ejecutó el justiciable, los momentos en que los hizo y su actitud una vez realizada la alteración del sistema dan cuenta de que aquel sí tenía el conocimiento del acto ilícito que se ejecutaba, que dentro del plan de autor tenía una función asignada y que esta no era baladí, sino esencial para el desarrollo de la actividad criminal.** Debe comprenderse que, en este tipo de asuntos, en donde **el suministro de una cuenta bancaria es un aspecto esencial, dentro del plan de autor, para llevar a cabo el fraude informático en sistemas bancarios digitales, puesto que solo con esta podría darse el traslado de fondos fraudulentos, desde una cuenta de origen a la cuenta de destino, para materializar el beneficio patrimonial que se procura o se obtiene,** debe analizarse cada caso concreto, para determinar si la prueba indiciaria permite verificar el dolo del prestatario de la cuenta y su participación dentro del plan de autor con dominio funcional junto con quien realiza la intrusión fraudulenta en el procesamiento de los datos, o si se carece de este elemento subjetivo. Más **resultaría inaceptable, como parece aducirlo la defensa pública, que la sola ausencia de prueba directa sea un límite para determinar la responsabilidad penal de este tipo de personas**, sino que lo que exige es un mayor esfuerzo de investigación y de valoración probatoria para lograr deducir de los indicios el dolo de autor o la ausencia de este. Como supra se explicó, en el presente asunto el dolo del imputado en una participación conjunta con el autor material de la intrusión informática, permiten determinar que la participación del endilgado fue en calidad de coautor funcional del hecho.” (Tribunal de Apelación de Sentencia Penal II Circuito Judicial de San José, Resolución Nº 1838 – 2022)

Así los hechos, se considera sumamente atinado el análisis intelectivo, probatorio y fáctico que exige el Tribunal de Apelación de Sentencia Penal en el voto supra transcrito, en relación con los elementos subjetivos del tipo penal. De lo contrario, se estaría contribuyendo a la impunidad del delito de estafa informática, sobre la base de una falta de análisis.

2. Formas de aparición del delito de estafa informática

2.1. Consumación y tentativa. Momento consumativo en la estafa informática.

Según Francisco Castillo, en su libro Estafa Informática (2016), el delito que ocupa el presente trabajo es un delito de resultado, que se consuma cuando se produce (total o parcialmente) el perjuicio patrimonial. Sin embargo, el mismo autor en su artículo de Homenaje a Javier Llobet titulado La estafa informática de "*Lege lata*" y de *"lege ferenda"* parece indicar que el delito podría perfeccionarse antes de la materialización del perjuicio patrimonial, en tanto afirma que "el texto vigente de la estafa informática del artículo 217 bis Código Penal no establece como requisito para la consumación la causación del perjuicio patrimonial" (2020: 298).

Por su lado, Calderón (2021) consideró que "llama la atención es que, el delito de *estafa general es un delito de resultado*, mientras tanto el de estafa informática incorpora dos posibilidades, sanciona al sujeto activo que "procure" u "obtenga", es decir, se trata de una mixtura, convirtiéndose en una construcción legislativa sui géneris, ya que es de resultado y de peligro, ante ese panorama, en acatamiento a los lineamientos de un sistema penal garantista, consideramos que la estafa informática prevista en el numeral 217 bis del CP, debería entenderse como un delito de resultado, de manera que posibilite la existencia de la tentativa".

Es criterio de quien redacta que **el momento configurativo en el delito de estafa informática se verifica apenas se lesiona el bien jurídico tutelado** (cfr. a la subsección supra de bienes jurídicos tutelados en el delito de estafa informática) **sin que sea necesario verificar la existencia de un beneficio consolidado para el autor**. Se coincide con la tesis de Castillo, considerando que se debe ir más allá. Mas no se comparte la de Calderón, pues una cosa es el perjuicio patrimonial o indebido y otra lo es el beneficio.

El texto del artículo 217 bis impone prisión a quien, en perjuicio de una persona física o jurídica realice los verbos típicos y sus modalidades, con la cual procure u obtenga un beneficio patrimonial o indebido para sí o para otro. Calderón (2021) parte de un momento de consumación del delito según el beneficio que "procure" u "obtenga" el sujeto activo, hablando de una dualidad de peligro / resultado. Sin embargo, el fin que mueve al autor (procurar u obtener un beneficio patrimonial o indebido) es un elemento subjetivo distinto del dolo, como recién se acaba de explicar. Y esta motivación que tiene el agente activo a la hora de cometer el delito (el procurarse u obtener un beneficio patrimonial o indebido) no se relaciona ni influye con el momento de perfección del delito.

El delito de estafa informática se perfecciona cuando se usa, manipula, influye o incide en los datos, en perjuicio de una persona física o jurídica. Es decir, si en ese uso, manipulación, incidencia o influencia de datos existe, entonces el objetivo de procurarse u obtener un beneficio patrimonial o indebido no es necesario para que se perfeccione el delito. Y esto no lo convierte en un delito de peligro (como afirma Calderón), en el tanto ya se lesionó en perjuicio de una persona física o jurídica su patrimonio u otro bien jurídico tutelado por el tipo penal.

Entonces, es criterio de quien redacta que, Castillo (2016) tiene una posición acertada, el tipo penal se consuma cuando se afecta el bien jurídico tutelado, pero se admite en esta tesis que, el tipo de estafa informática es pluriofensivo (cfr. sección de bienes jurídicos tutelados), razón por la cual, en el momento en el que se afecta la autonomía de los datos o el patrimonio de la persona ofendida, ahí es donde se tiene por configurado el delito.

No hay que olvidar que, atendiendo a categorías dogmáticas, hay una diferenciación espaciotemporal entre la acción y el resultado, que no incide en el beneficio que obtenga o procure su autor. Pues se debe tener claro que la consumación tiene lugar cuando se afecta el bien jurídico tutelado por la norma y no cuando se consigue el elemento subjetivo distinto del dolo. Si ya tuvo lugar la afectación, el tipo estará consumado.[7]

Con claridad en el momento en el que se consuma el delito, inherentemente se debe analizar ahora la tentativa, y si el delito de estafa informática permite la tentativa.

2..2. ¿Admite tentativa la estafa informática?

Para determinar cuando estamos en presencia de la figura de la tentativa, se han formulado diversas tesis dogmáticas. La Sala de Casación Penal en el voto 1104-2006, expone criterios orientan este análisis: desde la tesis carrariana de la univocidad de los actos, pasando por la formal objetiva -que considera iniciado el delito cuando el autor penetra en el núcleo del tipo-, la tesis material objetiva -que incorpora el para el bien jurídico tutelado- hasta llegar a la tesis individual objetiva, que actualmente predomina.

Según esta última tesis (individual objetiva), la Sala de Casación penal, en el voto de cita, ha argumentado que el análisis debe centrarse en **el plan del autor, y si según ese plan, la acción representa un peligro cercano para el bien jurídico tutelado.**

Se eligió por parte de la Sala de Casación la **tesis individual objetiva** por considerar que, sin llegar a la amplitud de la tesis subjetiva ni a la estrechez de la objetiva, es la que con mayor precisión

[7] En su curso de Penal Especial, en la maestría de ciencias penales, Manuel Rojas (2022) ejemplificaba el momento consumativo de los delitos con la afectación de bien jurídico al tipo más evidente: el homicidio. En donde a posteriori del homicidio, se realiza un desmembramiento del cuerpo para ocultarlo. Dicho desmembramiento no forma parte del homicidio, que tiene lugar con la muerte de la víctima.

establece los linderos: “Esta teoría se mantiene en el plano de lo objetivo en cuanto parte de la consideración de la conducta típica particular (teoría formal-objetiva), introduciendo un elemento individualizador (subjetivo), como el plan del autor, pero que por su naturaleza es susceptible de ser valorado por un tercero en cuanto a la determinación de la “proximidad inmediata” a la realización típica” (Voto de la Sala de Casación Penal 1043-2000 de 9:20 horas del 8 de setiembre del 2000).

A efectos de analizar la posibilidad o no de adelantar esta barrera punitiva en el delito de estafa informática, como bien se indicó en la sección anterior, se coincide con el criterio de Castillo (2016), se trata de un delito de resultado. Pues su configuración requiere la alteración del objeto material sobre el que recae la acción. Por tanto, hay una diferenciación espacio-temporal entre la acción y el resultado (el uso, manipulación, influencia o incidencia de los datos) y el obtener el beneficio patrimonial o indebido (que como se indicó en la sección previa, no es el momento de consumación del delito, sino un elemento subjetivo distinto del dolo).

Se considera entonces que la construcción típica del delito de estafa informática sí admite tentativa, y que esta se ubica en la fase externa del íter críminis, entre los actos de ejecución y los actos de consumación. Solo a partir de los actos encaminados a la ejecución del delito (el uso, manipulación, influencia o incidencia de los datos), pero antes de que se materialicen los resultados requeridos en la tipicidad objetiva -por causas ajenas a la voluntad del agente.

El análisis debe realizarse de forma casuística; empero, conforme a la tesis plasmada por la Sala de Casación Penal, cuando el examen de los elementos subjetivos del tipo penal permite evidenciar el dolo de la persona imputada de manipular, influir o incidir en los datos de la persona ofendida, resulta procedente valorar la existencia de la tentativa. En ese sentido, y sin perjuicio del necesario estudio casuístico, se sostiene que la redacción del tipo penal permite admitir la figura de la tentativa en el delito de estafa informática.

2.4. Concursos

Si bien se ha tratado de dejar claro que la comisión de la estafa informática permite no solo un perjuicio patrimonial antijurídico sino un beneficio indebido sin necesidad de que sea de índole patrimonial, lo cierto del caso es que en la especie lo más común en la jurisprudencia ha sido su configuración por el desplazamiento antijurídico patrimonial de dinero en cuentas bancarias mediante sistemas bancarios electrónicos.

Así los hechos, en el tema de concursos, Francisco Castillo (2016) ha sido adamante en establecer que si el mismo daño patrimonial es causado por diferentes modalidades de acción del artículo 217 bis (por ejemplo, por una indebida configuración del programa y por el empleo

de datos incompletos) solamente existe un hecho punible. Del mismo modo, existe también un solo hecho punible en el caso de que en un corto lapso de tiempo se saque de un cajero automático una gran cantidad de dinero, o cuando se hacen varias transacciones fraudulentas.

Relacionado con el concurso aparente de delitos entre la estafa informática y otras figuras, mediante resolución N° 00851-2017 del doce de julio de dos mil diecisiete el Tribunal de Apelación de Sentencia Penal del Primer Circuito Judicial de San José señaló:

> (…) la conducta a grandes rasgos se adecua a lo establecido en el numeral 373, relacionado con el 375 y 372, todos del Código Penal, empero la prioridad de aplicación de éstas normas, decae, cuando el ordenamiento jurídico cuenta con un tipo penal mas (sic) específico o especial, y es lo que en éste caso sucede, con relación al delito del numeral 217 bis, titulado como fraude informático (sic) […] De allí que el Tribunal tenía por imperativo de ley, el tipo especial, "fraude informático" y no "valor falso equiparado"(…)

En la resolución transcrita, el Tribunal se decanta por aplicar el tipo penal de estafa informática (otrora fraude informático) por su especialidad, pues si bien los artículos 372, 373 y 375 del Código Penal (falsificación de moneda, o valores equiparados) se encuentran en el Título XVI denominado "Delitos contra la fe pública", la estafa informática del numeral 217 bis se ubica en el Título VII de "Delitos contra la propiedad". Ésta última en su redacción, como factor normativo, no sólo es especial, también integra a los primeros tres, por lo tanto, nos encontramos ante un **concurso aparente de normas por criterio de especialidad y de consunción** según el artículo 23 del Código Penal, que es lo que al fin y al cabo aplicó, sin decirlo el Tribunal de Apelación de Sentencia Penal del Primer Circuito judicial de San José (Calderón, 2021).

3. Penalidad del delito de estafa informática

La pena que sanciona la estafa informática puede distinguirse en la pena simple (prisión de tres a seis años) y la pena agravada (prisión de cinco a diez años).

7.1. Pena Simple

Para la estafa informática simple el legislador dispone prisión de tres a seis años. La pena indicada puede parecer inadecuada por ser demasiado elevada cuando se trata de estafas informáticas insignificantes (lo cual como se analizará en la segunda parte, en múltiples ocasiones parece llevar a criterios de oportunidad) o puede parecer relativamente benigna cuando se trata de estafas informáticas muy elaboradas que produzcan un gran daño económico-social. Lo anterior contrasta con la penalidad que tiene el delito de estafa "básica"

simple (216 Código Penal), en el cual el legislador escalona la pena de dos maneras: prisión de dos meses a tres años, si el monto de lo defraudado no excediere diez veces el salario base, y prisión de seis meses a diez años, si el monto de lo defraudado excediere de diez veces el salario base.

Respecto a la estafa del artículo 216 agravada, cuando se dan algunas de las circunstancias agravantes, las penas previstas para la estafa menor y para la estafa mayor se elevan en un tercio. Indica Castillo (2016) que una pena fija como la utilizada por el legislador en el artículo 217 Código Penal puede resultar más injusta que el sistema de las cuantías que utiliza el artículo 216 Código Penal para la fijación de la pena; puesto que el régimen especial que tiene la estafa informática respecto a la estafa general no se justifica. Se comparte enteramente la posición de Castillo pues incluso en su modalidad simple, la dosificación de la pena podría ser desmedida en atención a estafas informáticas por montos ínfimos o que en atención a las circunstancias particulares del caso no generan un gravamen equiparable al quantum mínimo de la pena (tres años), lo cual, como se indicó podría operar también a la inversa.

7.2. Pena Agravada

El tipo penal reviste la modalidad agravada de comisión, la cual podemos denominar "estafa informática agravada", previendo una pena de prisión en abstracto que oscila entre los cinco a los diez años de prisión:

> si las conductas son cometidas contra sistemas de información públicos, sistemas de información bancarios y de entidades financieras, o cuando el autor es un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos. (Código Penal, 1970, 217 bis)

Entonces, la estafa informática en su forma de comisión simple prevé una pena mínima de tres años de prisión, y de cinco años en su modalidad agravada, extremos que están muy por encima de los mínimos de prisión previstos en abstracto en la estafa general: dos meses (pena base), dos meses y veinte días (pena base aumentada en un tercio), seis meses (pena agravada) y ocho meses (pena agravada aumentada en un tercio).

Se evidencia entonces, una desproporción importante en la dosificación penal, a pesar de que ambos tipos penales tutelan, en principio, el mismo bien jurídico. Sin embargo, las consecuencias procesales para quien deba descontar esas penas serán muy distintas, aun cuando se impongan los extremos mínimos, por ejemplo: la imposibilidad de optar por salidas alternas

como la suspensión del procedimiento a prueba y la conciliación (por exceder el extremo mínimo de tres o menos años según el artículo 25 y 36 del Procesal Penal), ante la modalidad agravada de la estafa informática, tampoco permite conceder el beneficio de ejecución condicional de la pena, previsto en el artículo 59 y siguientes del Código Penal[8].

Y, si se analiza que una de las causas por las cuales se agrava el delito de estafa informática, se presenta cuando la conducta es cometida en contra de sistemas de información públicos, sistemas de información bancarios y de entidades financieras, podríamos inferir prima facie, bajo el análisis de Calderón (2021), que esa es la modalidad de comisión más frecuente, convirtiendo la agravante en regla y no en excepción. Ahora, en la segunda parte de esta investigación se realizó un estudio estadístico de causas penales que permiten anticipar esta afirmación sobre la modalidad de comisión más frecuente.

Vale mencionar que la sola previsión en abstracto de un extremo menor de tres años de prisión, en la modalidad simple del delito de estafa informática, pone en riesgo la posibilidad de optar por el beneficio de ejecución condicional de la pena, por cuanto el mínimo aumento que pueda ser aplicado por el Tribunal de sentencia, por ejemplo, un día, cercena definitivamente la aplicación de ese instituto. Diferente situación acontece ante el delito de estafa general, ya que aun y cuando, el Tribunal sentenciador eleve las penas mínimas, por ejemplo, en otro tanto, ni siquiera se acerca al límite establecido como requisito para la precedencia del beneficio mencionado.

Es decir, el margen de actuación que tiene la persona juzgadora en la dosificación de la pena es mayor en el delito de estafa general, sin afectar la posibilidad de otorgar el beneficio de ejecución o incluso la posibilidad de medidas alternas en etapas previas.

No se omite mencionar que, en cuanto al extremo mayor de pena previsto en abstracto, la situación se invierte, toda vez que, la estafa general prevé una pena máxima de trece años y tres meses de prisión, según lo establecido en el último párrafo del artículo 216 del Código Penal, mientras tanto, la estafa informática prevé como extremo mayor diez años de prisión en su forma de comisión agravada.

Analizado lo anterior, se destaca otro desfase legislativo en el *quantum* de una eventual pena, pues si bien la estafa informática en su extremo mayor prevé una penalidad inferior, lo cierto es que, el extremo inferior en la pena mínima en abstracto para la estafa informática es más perjudicial. Se entrevé que se considera a la estafa informática como un delito resguardado

[8] El artículo 59 del Código Penal indica: "Condena de ejecución condicional. Al dictar sentencia, el Juez tendrá la facultar de aplicar la condena de ejecución condicional cuando la pena no exceda de tres años y consista en prisión y extrañamiento."

con penalidades más severas en sus extremos inferiores, pero no en sus extremos superiores "techos", lo cual carece de todo sentido.

Este desfase se acentúa aún más cuando se analiza que es a partir de ese "piso" (el extremo mínimo) que los juzgadores se ven obligados a imponer una pena (pues del extremo mínimo se parte para definir el *quantum* de la pena y no a la inversa).

Así los hechos, al confrontar las penas asignadas en el artículo 217 bis del Código Penal con su homónimo 216, logramos derivar que quienes legislaron, consideraron más reprochable, por lo menos en cuanto a su extremo mínimo de punibilidad, las conductas de la estafa informática por sobre la de la estafa "básica". Esto incluso a pesar de que ambas figuras protegen el bien jurídico patrimonio, y que "la estafa general, tiene secuelas más severas en la persona física que se convierte en víctima, no sólo desde un punto de vista de su patrimonio, sino más importante, desde aspectos emocionales" (Calderón 2021: 67).

Como se adelantó, se considera que este desfase legislativo no es razonable, si se protege como bien jurídico "principal" en ambas el patrimonio se considera que sus penas debieron ser equiparadas a efectos de no generar inconsistencias en el *quantum* y el reproche que se pueda generar desde la imposición de la pena. O asignar mínimos y máximos coherentes con el reproche que se pretende en cada una de ellas. Pues, tal y como se encuentran estipuladas en la actualidad, devienen en incoherentes entre sí, atendiendo la armonía normativa que debe imperar en el ordenamiento jurídico.

Finalmente, véase que, de todos los delitos informáticos vigentes en nuestro ordenamiento jurídico, la estafa informática es uno de los que tiene mayor penalidad prevista en abstracto, circunstancia que refleja el interés del legislador, en "proteger" mediante leyes, de manera más estricta el patrimonio[9], que otros derechos de las personas, como la intimidad, privacidad e incluso la autodeterminación informativa (Calderón, 2021), y si se analiza con los demás tipos penales patrimoniales, es el tipo penal (sin proscribir violencia física) que protege el patrimonio con la dosificación penal más alta.

[9] Ver en este sentido a Christian Fernández Mora. *La racionalidad tecnológica de la justicia penal en Costa Rica y su (Des) Humanización.* Revista Digital de la maestría en ciencias penales de Universidad de Costa Rica. Homenaje al Prof. Dr. Francisco Castillo González en sus 70 años. N° 5, ISSN: 1659-4479, 2014, pp. 126 y 127: "*Se trata, más bien, de una clara fachada de lo humano que es la justicia –no en su sentido ideal, sino en el sentido real o material- cuando pretende llevar hasta sus límites máximos la idea de la modernidad, de una racionalidad marcada por las reglas del mercado, donde las prácticas más democráticas se vuelven formas de sometimiento. Por eso Foucault señala que las democracias actuales, nos permiten vivir "…bajo un régimen de dictadura de clase, de un poder de clase que se impone a través de la violencia, incluso cuando los instrumentos de esta violencia son institucionales y constitucionales"*

Segunda parte: Evaluación empírica de la respuesta penal a la estafa informática en la fase preparatoria e intermedia (2020-2023)

Analizado que fue el tipo penal de forma teórica, se consideró indispensable indagar, desde una perspectiva empírica, la manera en que dicho delito es investigado por el Ministerio Público en Costa Rica. En este sentido, la hipótesis de trabajo -según la cual el delito de estafa informática no está siendo investigado efectivamente por el Ministerio Público, lo que propicia escenarios de impunidad- fue trasladada a un enfoque de investigación cuantitativa[10] de diseño metodológico muestral intencionado[11] (Bryman, 2012) también llamado muestreo de conveniencia[12].

Esta hipótesis fue sometida a prueba mediante la selección de una muestra no aleatoria (Bryman, 2012 y Tamayo 2004) compuesta por 100 causas penales tramitadas bajo el delito de estafa informática. Se tomó esa muestra y se analizó bajo un modelo de regresión múltiple con un examen de validez y un modelo de mínimos cuadrados ordinarios, con el objetivo de verificar, refutar o matizar la hipótesis planteada. En particular, determinar si, el artículo 217 bis del Código Penal —norma que busca brindar una protección reforzada al patrimonio en el contexto digital— se aplica efectivamente en la realidad judicial costarricense, o si, por el contrario, se configura como una disposición normativa vacía de contenido, lo que a su vez validaría la hipótesis sobre la falta de investigación y consecuente impunidad del delito.

Así los hechos, el análisis del muestreo intencionado, partió de la información dada por la Dirección de Planificación del Poder Judicial[13], bajo el permiso otorgado a la investigadora por parte del Consejo Superior de la Corte Suprema de Justicia en sesión N° 33-2022 celebrada el 21 de abril de 2022, artículo XVI.

Esta base de diagnóstico reveló que, en 2020, 2021 y 2022 se tramitaron 16 672 casos por el delito de estafa informática en todo el territorio nacional (los datos del 2023 no estaban disponibles para el momento de investigación). De los cuales 7775 casos se tramitaron en San José (46.6%); 2760 causas penales se tramitaron en Limón (16.5%); 1933 causas penales se tramitaron en Alajuela (11.6%); 1632 causas penales se tramitaron en Puntarenas (9.8%); 1120 causas penales se tramitaron en Cartago (6.7%); 953 causas penales se tramitaron en Guanacaste (5.7%); y 498 causas penales se tramitaron en Heredia (3.0%).

[10] Ver supra nota 2.
[11] Ver supra nota 3.
[12] Ver supra nota 4.
[13] Ver supra nota 5.

Como se justificó en el marco metodológico, la investigación empírica se enmarcó territorialmente en el Primer Circuito Judicial de Alajuela (selección del parámetro geográfico analizado) pues es el circuito judicial que por competencia territorial analiza las estafas informáticas presuntamente ejecutadas desde los centros penales (comúnmente conocidos como "call centers" penitenciarios). Además de su relevancia temática, se eligió dicho circuito por ser el tercero con mayor cantidad de causas por estafa informática a nivel nacional, y por razones de imparcialidad metodológica, en virtud de que quien suscribe esta tesis ejerció funciones jurisdiccionales en los circuitos judiciales de San José y Limón durante el período temporal analizado.

Temporalmente (sobre la selección del parámetro temporal utilizado) se analizaron las causas penales tramitadas en dicho despacho desde enero de 2020 hasta agosto de 2023 inclusive, fecha de corte correspondiente a la redacción del presente trabajo. Pues como se indicó en los antecedentes, Calderón Chaves en su trabajo final de investigación aplicada para optar al grado y título de Maestría Profesional en Ciencias Penales (2021) analizó el tratamiento jurisprudencial de la estafa informática en Costa Rica durante los años 2014 al 2019 por parte de Sala Tercera (sic) y el Tribunal de Apelación de Sentencia Penal del Primer Circuito Judicial de San José. Concluyendo que en todo ese periodo se dictaron solamente veintiún resoluciones por parte de Sala Tercera (sic) sobre el tema y, "si bien el TASP emitió mayor cantidad de resoluciones en comparación a la Sala Tercera (sic), los análisis de fondo con respecto al tipo penal fueron laxos" (Calderón 2021: 212).

Los hallazgos de aquella investigación justificaron la necesidad de ahondar y retrotraerse a etapas previas del proceso penal -etapa preparatoria e intermedia-, a efectos de averiguar no solo si el resultado de la investigación de Calderón tiene su problema en etapas previas, como se sospechaba, sino también aceptar como válida o refutar la hipótesis de esta investigación, generando la necesidad de un análisis cuantitativo.

1. Análisis cuantitativo de causas penales sometido a un Modelo de Regresión Múltiple

A efectos de verificar la hipótesis de trabajo, se siguió un método empírico respaldado por el principio de validez interna de la medición propuesto por Bryman (2012). Este se centra en determinar si una relación causal entre dos o más variables es sostenible. Es decir, si puede afirmarse con rigor que la variable independiente (X) incide sobre la variable dependiente (Y) sin que dicha asociación esté mediada o distorsionada por otros factores no controlados. En

este contexto, la validez interna constituye una herramienta crítica para evaluar si los efectos observados son atribuibles con certeza a las variables explicativas del modelo.

Con base en este marco de Bryman (2012), se aplicó un modelo de regresión múltiple utilizando el método de estimación por Mínimos Cuadrados Ordinarios (MCO), con el objetivo de analizar el grado de incidencia de ciertos factores institucionales y procesales en la investigación del delito de estafa informática en la etapa preparatoria e intermedia del proceso penal. Este enfoque permitió evaluar empíricamente la asociación entre distintas variables independientes —vinculadas con la actuación o inacción de los operadores del sistema penal— y la persistencia de resultados procesales que reflejan la ausencia de persecución efectiva del delito,[14]

En los apartados siguientes, se detallan los resultados del análisis estadístico, incluyendo los coeficientes obtenidos, su significancia, el grado de ajuste del modelo y los indicadores de validez interna, con el propósito de ofrecer una interpretación empíricamente fundada sobre la sospecha de impunidad en los casos de estafa informática.

Justificación Socio-Jurídica del análisis

Antes de presentar los resultados del análisis estadístico, fue necesario cuestionar si la hipótesis (según la cual el Ministerio Público no investiga los delitos de estafa informática, lo cual genera impunidad) incorpora una relación causal entre variables que pueda ser verificada empíricamente. Esto, por cuanto, si se sugiere que la falta de investigación del Ministerio Público *es* lo que causa la impunidad, se debe cuestionar si es posible afirmar categóricamente lo anterior, sea: **¿Se puede asegurar que el Ministerio Público es el responsable de la variación en la impunidad del delito de estafa informática y no otro factor que esté produciendo una relación causal aparente?**

Por esta razón, el análisis de la **variable independiente** (los predictores, aquella que se manipula, se cree que afecta o influye en la variable dependiente), se enfocó en los actos de investigación en la etapa preparatoria y conclusivos en la intermedia que afectan directamente a la afirmación de que el delito de estafa informática no está siendo investigado y existe impunidad (variable dependiente).

[14] El modelo se formuló tomando como referencia los principios metodológicos y estadísticos expuestos en el material didáctico del curso Matemáticas y estadísticas: *Análisis Múltiple de Datos*, impartido por la Universitat Oberta de Catalunya (2022)

Pues, podrían existir factores exógenos al impulso del Ministerio Público (se podría argumentar especulativamente la falta de interés de las víctimas, por ejemplo) que eximan al órgano fiscal de esta impunidad. Factores que, desde luego, también fueron analizados.

Por su parte, la variable dependiente (Y) (Y) es la impunidad en causas por estafa informática y, como variable independiente (X) los factores relevantes que afectan la impunidad del filtro del muestreo intencional no aleatorio[15] enfocados en los factores que afectan la investigación.

Siendo los siguientes:

(1) el OIJ: si el OIJ realizó actos de investigación en dicha causa; si así lo hizo, entonces cuáles actos de investigación realizó y plasmó en el informe inicial; si le solicitó al Ministerio Público gestionar actos de investigación ante el juzgado penal y cuáles; (2) el Ministerio Público: si el Ministerio Público acogió la solicitud del OIJ y solicitó al Juzgado Penal actos de investigación; si así fue, cuáles; si en la causa penal existía persona imputada individualizada o si por el contrario era contra ignorado; se plasmó el acto conclusivo del órgano fiscal y su fundamento para llegar a ese acto conclusivo. (3) El juez: el acto resolutivo del juez penal y su fundamento. Y finalmente, (4) La víctima, entiéndase la participación o colaboración de la propia víctima en la investigación penal.

Para tener las siguientes:

- **Variable Dependiente (Y)**: es la impunidad en casos de estafa informática.
- **Variable Independiente (X1)**: Falta de investigación del **Organismo de Investigación Judicial (OIJ)**.
- **Variable Independiente (X2)**: Falta de investigación del **Ministerio Público**.
- **Variable Independiente (X3)**: **Falta de cooperación de la víctima**
- **Variable Independiente (X4)** Participación del **juez penal**.

Con base en estos elementos, la relación de estas variables en el modelo de regresión adoptó la siguiente fórmula:

$$Y = \beta\,0 + \beta\,1\,X\,1 + \beta\,2\,X\,2 + \beta\,3\,X\,3 + \beta\,4\,X\,4 + \varepsilon \quad Y=\beta\,0\ +\beta\,1\ X\,1\ +\beta\,2\ X\,2\ +\beta\,3\ X\,3\ +\beta\,4\ X\,4\ +\varepsilon$$

[15] Los efectos de un muestreo intencional no aleatorio se basan en el conocimiento de la persona investigadora para generar muestras representativas. En este caso, el muestreo no aleatorio procuró seleccionar las causas penales más representativas del 2020 – 2023, es decir, que permitieran mostrar ejemplificativamente un porcentaje representativo de la totalidad de los requerimientos conclusivos mayormente ejecutados por la Fiscalía de Alajuela.

En esta fórmula, el valor β_0 representa el valor base de impunidad cuando no hay inacción atribuible a ninguno de los operadores. Los coeficientes β_1 a β_4 indican cuánto cambia la impunidad ante la variación de cada uno de los predictores, controlando por los demás. Y también se incluyó el término de error (ε), representa todo aquello que puede estar influyendo en la impunidad pero que no fue incluido en el modelo, como factores externos no observados. Más claro:

- Y representa la impunidad (variable dependiente).
- X_1 representa la falta de investigación del OIJ.
- X_2 representa la falta de investigación del Ministerio Público.
- X_3 representa la participación de la víctima.
- X_4 representa la participación del juez penal.
- ε es el término de error.

Se estimó este modelo mediante el método de Mínimos Cuadrados Ordinarios (MCO), el cual permite identificar qué variables tienen una relación estadísticamente significativa con la impunidad en el delito de estafa informática. En el *Anexo I* se incluye el detalle de cada causa penal analizada, así como las variables, sistematización y hallazgos estadísticos obtenidos.

Como parte del análisis, se llevó a cabo una **evaluación del modelo,** en la que se calculó un indicador que muestra qué proporción de la variación en los niveles de impunidad puede ser explicada por las variables independientes analizadas.

Asimismo, se aplicaron **pruebas de hipótesis**, para determinar si los coeficientes de las variables independientes son estadísticamente significativos. Esto permitió identificar cuáles de los sujetos considerados —el Organismo de Investigación Judicial, el Ministerio Público, la víctima y el Juzgado Penal— inciden de manera comprobable en la generación de impunidad en casos de estafa informática.

Además, para dotar de validez estadística los resultados, se realizó una **revisión de los residuos del modelo**. Es decir, de las diferencias entre los valores reales observados y los valores que el modelo predice. Esta revisión es fundamental para verificar que se cumplen ciertos **supuestos básicos del modelo de regresión**, como que los errores (residuos) estén distribuidos de forma aleatoria, con una varianza constante y sin patrones sistemáticos. Esto asegura en una investigación estadística, que el modelo no solo se ajusta bien a los datos, sino

que lo hace de manera **fiable y sin sesgos ocultos** que pudieran invalidar las conclusiones. Esta verificación brinda mayor solidez a la interpretación de los resultados obtenidos.

Con base en todo lo anterior, se presentan los resultados clave del modelo:

Estadísticas de Regresión

Múltiple R	0,91087582
R cuadrado	0,82969477
R cuadrado ajustado	0,82063598
Error Estándar	0,18897023
Observaciones	100

ANOVA

	df	*SS*	*MS*	*F*	*Signifi F*
Regresión	5	16,353283 9	3,27065677	91,5900318	1,4141E-34
Residual	94	3,3567161 3	0,03570975		
Total	99	19,71			

	Coeficientes	*Error Estándar*	*Estad T*	*P-valor*	*Bajo 95%*	*Alto 95%*	*Bajo 95,0%*	*Alto 95,0%*
Intercepto	0,97636722	0,0860257 9	11,3497038	2,5913E-19	0,805561	1,14717344	0,805561	1,14717344
X1 (¿OIJ investigó?)	0,04585198	0,0646596 5	0,70912816	0,48000009	-0,082531 3	0,17423523	-0,082531 3	0,17423523
X2 (¿MP INVESTIGÓ?)	0,03856571	0,0441148 3	0,87421199	0,38423087	-0,049025 3	0,12615673	-0,049025 3	0,12615673
x3 (Fundamento MP)	0,08750527	0,0156579 5	5,58855068	2,2258E-07	0,056416 04	0,11859451	0,056416 04	0,11859451
x4 (¿VÍCTIMA COOPERÓ?)	0,04985 84	0,0529563 5	0,94150006	0,34886199	-0,055287 7	0,15500448	-0,055287 7	0,15500448

X5 (Participación JP)	-0,3407924	0,02350184	-14,500671	1,0383E-25	-0,3874559	-0,294129	-0,3874559	-0,294129

(Tabla 1, Modelo de Regresión múltiple de impunidad en el delito de estafa informática. Elaboración propia)

2. Interpretación y análisis de resultados

El modelo de regresión múltiple aplicado identificó qué factores institucionales o procesales inciden en los niveles de impunidad en casos de estafa informática. Se analizaron cinco variables independientes relacionadas con la actuación del OIJ, del Ministerio Público, de la víctima y del Juzgado Penal.

La evaluación del modelo mostró que la proporción de variabilidad en la impunidad que puede ser explicada por las variables analizadas es del 82%. Este resultado indica que el modelo tiene un alto poder explicativo: las variables seleccionadas permiten describir muy bien el comportamiento de la impunidad en el conjunto de casos estudiado (este resultado se desgrana del R cuadrado ajustado)

De forma más técnica, el R cuadrado ajustado (también conocido como coeficiente de determinación ajustado); es la métrica utilizada en las regresiones múltiples para evaluar qué tan bien se ajusta el modelo a los datos, y determinar qué variables son relevantes. El R cuadrado ajustado es una versión modificada del R cuadrado (coeficiente de determinación) que tiene en cuenta la cantidad de variables independientes en el modelo. El R cuadrado (R^2), también conocido como coeficiente de determinación mide la proporción de la variabilidad total en la variable dependiente que se explica por el modelo. En otras palabras, R^2 nos dice qué porcentaje de variación de la variable dependiente es explicado por todas las variables independientes juntas. Si $\mathbf{R^2}$ es cercano a 1, significa que las variables independientes explican una gran parte de la variabilidad en la variable dependiente. Ahora, mientras que el R cuadrado simplemente mide la proporción de la variabilidad total explicada por el modelo, el R cuadrado ajustado penaliza la inclusión de variables irrelevantes. Los resultados del caso en estudio fueron:

Multiple R	0,91087582
R cuadrado	0,82969477
R cuadrado ajustado	0,82063598

El R cuadrado ajustado varía entre 0% y 100%: un valor cercano al 0% indica que el modelo no explica bien la variabilidad en la variable de respuesta. Un valor cercano al 100% indica que el modelo se ajusta muy bien a los datos.

En el caso de estudio, el R cuadrado ajustado es 0.8206. Esto significa que aproximadamente el 82.% de la variabilidad en la impunidad de casos de estafa informática se explica por las variables independientes incluidas en el modelo. O sea, **las variables independientes analizadas en esta investigación son excelentes para predecir los factores que afectan la impunidad en el delito de estafa informática**.

Sobre los factores que afectan la impunidad en el delito de estafa informática, el resultado del modelo de regresión múltiple revela que la actuación del Ministerio Público y la participación del Juzgado Penal tienen efectos estadísticamente significativos en la impunidad de la estafa informática. Entiéndase que, sin haber cuestionamiento sobre la existencia de un hecho ilícito de estafa informática, este no se investigó efectivamente. Así, la impunidad se entiende no solo como la ausencia de sanción, sino como la **falla sistémica en la administración de justicia, donde la falta de investigación y sanción de las personas responsables perpetúan la violación de derechos y la indefensión de las víctimas**. Los hallazgos son los siguientes:

- **Variables Significativas**:
  - x3 (Fundamento MP): Con un p-valor de aproximadamente 2.23E-07, esta variable es estadísticamente significativa, lo que indica que **el fundamento del Ministerio Público en su acto conclusivo tiene un impacto estadísticamente significativo considerable en generar impunidad del delito de estafa informática.**
  - X5 (Participación del JP): Con un p-valor extremadamente bajo de aproximadamente 1.04E-25, esta variable también es significativa y muestra que **la participación del Juzgado Penal tiene una influencia significativa en la reducción de la impunidad de la estafa informática.**

En contraste, las variables asociadas con la investigación por parte del OIJ (x1), la investigación del Ministerio Público (x2) y la cooperación de la víctima (x4) no presentaron una relación estadísticamente significativa con la impunidad, de acuerdo con los valores p obtenidos.

- **Variables No Significativas**:

- X1 (¿OIJ investigó?): Con un p-valor de 0.48, esta variable no es significativa, lo que sugiere que la falta de investigación del OIJ no impactó estadísticamente en la impunidad.
- X2 (¿MP investigó?): Con un p-valor de 0.384, tampoco es significativa, indicando que **no es relevante si Ministerio Público investiga o no, sino el acto conclusivo que ejecute con esa investigación**. Esta variable no tiene un impacto estadísticamente comprobable en la impunidad.
- x4 (¿víctima cooperó?): Con un p-valor de 0.349, esta variable tampoco es significativa, lo que sugiere que la cooperación de la víctima no tiene un impacto estadísticamente comprobable en la impunidad.

Lo anterior se desprende del análisis de los coeficientes y **los P-valores**. Los últimos explican si las relaciones entre las variables independientes y la variable dependiente son estadísticamente significativas. Un p-valor bajo (generalmente menor que 0.05) indica que la variable independiente tiene un impacto significativo en la variable dependiente y que es poco probable que el efecto observado sea debido al azar y, por lo tanto, la variable es estadísticamente significativa. Por su parte, los **coeficientes** representan el cambio esperado en la variable dependiente por cada unidad de cambio en la variable independiente, manteniendo todas las demás constantes. Un coeficiente positivo indica una relación directa con la variable dependiente; uno negativo indica una relación inversa (coeficiente negativo implica que este actor contribuye a la no impunidad, positivo contribuye a la impunidad).

Conclusiones

Amén del análisis que se hizo del tipo penal de estafa informática, así como del tratamiento que se le ha dado en Costa Rica en la etapa preparatoria e intermedia, es posible concluir lo siguiente:

1. **La estafa informática es un delito de creación relativamente reciente.** Su aparición surge en el marco de la sociedad de la información y de la universalización de las tecnologías digitales. En Costa Rica, surge como una modalidad de delito informático, a partir de la creación de la figura penal de fraude informático, que fue abiertamente criticada a nivel doctrinario y jurisprudencial, por no incluir todas las modalidades de comisión utilizadas en este tipo de acciones. En la reformulación al tipo penal actual, se

incluyó un nuevo verbo rector y se aumentó considerablemente la pena a imponer, entre otros cambios. Pese a ello, la modificación se vio motivada a nivel legislativo por inclinaciones de inmediatez y populismo, sin que existiera una adecuada fundamentación desde una perspectiva estadística, dogmática y criminológica. Esta inclinación populista afectó directamente a la capacidad de investigar el delito, pues constantemente se crean más y más tipos penales, sin robustecer al Poder Judicial, encargado de investigar, tramitar, juzgar y dar respuestas sobre la delincuencia.

2. **Existe debilidad argumentativa en las exposiciones de motivos que dieron origen a la regulación actual del delito de estafa informática, y en la precisión jurídica de los términos introducidos con la reforma generada por la Ley N.º 9048**. La ausencia de sustento empírico robusto, la falta de estudios criminológicos comparativos y el recurso a fuentes de baja rigurosidad —como entradas de Wikipedia o notas periodísticas— reflejan una tendencia legislativa preocupante: la apelación a discursos alarmistas y populistas para justificar reformas penales. Esta carencia de fundamentación técnica compromete la calidad normativa del tipo penal, y consecuentemente la precisión de la conducta punitiva que se pretende sancionar, agravando su ambigüedad al incorporar, dentro del artículo 217 bis, conductas de naturaleza heterogénea, como ciberdelitos en sentido estricto (dirigidos contra sistemas o datos informáticos) y delitos simplemente facilitados por tecnologías digitales. Esta inclusión indiscriminada conceptual y dogmáticamente generó un tipo penal mal estructurado, que dificulta su aplicación judicial y vulnera principios de legalidad. En consecuencia, se impone la necesidad de repensar el valor jurídico que se le otorga a las exposiciones de motivos, así como promover una cultura legislativa que privilegie el análisis criminológico serio, la coherencia sistemática del Derecho Penal y el rigor técnico como ejes fundamentales de la política criminal.
3. **Con la estafa informática en su redacción actual se violentan los subprincipios del artículo 39 constitucional sobre la legalidad penal.** Se incumplió con la obligación de acatar los subprincipios de *lex certa y lex stricta*: se creó un tipo penal abierto; sin armonía dentro del contexto del Código Penal, y con una denominación jurídicamente imprecisa (ya que se le denomina estafa sin ser propiamente una estafa, no guarda relación con la estafa convencional del artículo 216 del Código Penal, está precedido del delito de estelionato y no tiene relación alguna con este). También prevé una pena que no guarda coherencia con la estafa general; no hace diferencia con respecto al tema de la

cuantía de lo defraudado; su forma de comisión agravada es más frecuente que la simple; fue creado sin hacer un análisis adecuado de cuál era la necesidad de su existencia y en lo atinente a las modalidades de comisión, se redactó sin especificar precisa, clara y de forma circunstanciada cuál es la forma de comisión de la acción penal en esta última modalidad. Esto deja abierto al arbitrio de la persona juzgadora el encajar conductas no indicadas por el legislador dentro de esta modalidad. Aunque se diga que están sujetas a un resultado, el grado de incerteza e indeterminación jurídica que le acarrean no pasa los estándares mínimos de tipicidad legal establecidos por nuestra legislación.

4. **Sobre la impunidad en el delito de estafa informática**, el análisis de los datos del modelo de regresión múltiple realizado permite demostrar que, en el Primer Circuito Judicial de Alajuela, existen dos factores institucionales con incidencia estadísticamente significativa en la impunidad del delito de estafa informática. Sea,
    a. El fundamento de los actos conclusivos del **Ministerio Público** es el factor estadístico que **se asocia con la impunidad** del delito de estafa informática, desfavoreciendo la persecución penal efectiva del delito.
    b. En contraste, la participación del Juzgado Penal se vincula como factor en la **disminución de la impunidad** en los delitos de estafa informática.
5. Contrario a lo sospechado inicialmente, las variables correspondientes a la falta de cooperación de la víctima, la ausencia de investigación del OIJ y la falta de investigación del Ministerio Público no mostraron una relación estadísticamente significativa con la impunidad. Los resultados arrojaron que, no es la ausencia de investigación lo determinante, sino el tipo de acto conclusivo que se emite con base en dicha investigación. Estos hallazgos permiten relativizar ciertas creencias extendidas sobre la inacción investigativa como factor principal de impunidad, sugiriendo que el foco debe ponerse en la calidad de las decisiones del Ministerio Público y el Juzgado Penal.
6. A partir de los resultados empíricos, se confirmó la hipótesis de investigación: el delito de estafa informática no está siendo investigado de manera efectiva por parte del órgano fiscal, lo que genera un **escenario estructural de impunidad.** Este contexto evidenció debilidades institucionales que comprometen la capacidad del sistema judicial costarricense para abordar con eficacia esta modalidad delictiva.
7. El modelo utilizado no presentó indicios graves de heterocedasticidad (es decir, variación no constante del error aplicando la prueba de Breush-Pagan), ni tampoco evidenció multicolinealidad severa (correlaciones demasiado altas entre variables independientes que distorsionen la estimación de los coeficientes). Lo anterior permite concluir que el modelo

de análisis utilizado es confiable, que sus estimaciones son eficientes y se interpretó los coeficientes de manera robusta dentro de los límites de la muestra y del método.

8. El análisis efectuado evidenció una preocupante tendencia en la aplicación judicial del tipo penal de estafa informática. La falta de aplicación con precisión jurídica de los elementos objetivos y subjetivos del tipo penal de estafa informática llevó a que en múltiples expedientes analizados se equiparara indebidamente el artículo 217 bis con la estafa convencional del artículo 216 del Código Penal. Esta confusión no solo es técnicamente incorrecta, y deja entrever la falta de precisión terminológica de los operadores judiciales, sino que produce efectos nocivos sobre los derechos de las personas imputadas - ofendidas y sobre la coherencia del sistema penal en su conjunto. Se requiere formación especializada y una mayor claridad dogmática en torno a los elementos normativos y materiales que configuran este tipo penal.
9. Pese al panorama crítico que revela el análisis teórico y empírico, la investigación pone de relieve oportunidades concretas de mejora institucional. Los hallazgos apuntados permiten ubicar con nitidez los puntos neurálgicos en el tratamiento judicial de la estafa informática, constituyendo el primer paso para el diseño de estrategias más eficaces, tanto desde la práctica judicial como desde el diseño legislativo. Reconocer estas debilidades no debe concebirse como un ejercicio pesimista, sino como un imperativo de fortalecimiento interinstitucional, orientado a mejorar la calidad de la tramitación y las decisiones judiciales, consolidando así una administración de justicia más coherente, informada, efectiva y respetuosa de los principios del derecho penal democrático.

Bibliografía consultada

Normativa

Constitución Política (1949). *Constitución Política de la República de Costa Rica*. La Gaceta, n.º 252.

Ley N.º 3394 (1964). *Convención de Viena sobre Relaciones Diplomáticas*. La Gaceta, n.º 238.

Ley N.º 4573 (1970). *Código Penal.* La Gaceta, n.º 257.

Proyecto de Ley N.º 14.079 (2000). *Reforma de los artículos 215, 272 y 372 del Código Penal*. La Gaceta, n.º 192.

Proyecto de Ley N.º 14.782 (2002). *Reforma de los artículos 191, 192 y 215 del Código Penal, Ley N.º 4573*. La Gaceta, n.º 124.

Proyecto de Ley N.º 17.009 (2008). *Ley para el fortalecimiento de la legislación contra el terrorismo.* La Gaceta, n.º 86.

Tratado Internacional N.º 8302 (2002). *Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y sus Protocolos (Convenio de Palermo, 2000).* La Gaceta, n.º 123.

Tratado Internacional N.º 9452 (2017). *Convenio de Europa sobre Ciberdelincuencia (Budapest, 2001).* La Gaceta, n.º 125.

Doctrina

Aboso, G. (2017). *Derecho penal cibernético: La cibercriminalidad y el derecho penal en la moderna sociedad de la información y la tecnología de la comunicación*. Euros Editores S.R.L.; Editorial BdeF Ltda.

Aguilar, J. (2020). *La brecha de ciberseguridad en América Latina frente al contexto global de ciberamenazas. Revista de Estudios en Seguridad Internacional*, *6*(2), 17–43. https://dialnet.unirioja.es/servlet/articulo?codigo=7716111

Barmpaliou, N. (2020). *Amenazas emergentes en ciberseguridad: Implicaciones para América Latina y el Caribe. En Banco Interamericano de Desarrollo (Coord.), Reporte de ciberseguridad 2020* (pp. 28–33).

https://publications.iadb.org/publications/spanish/viewer/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Borja, E. (1995). La terminación del delito. *Anuario de Derecho Penal y Ciencias Penales, 48*(1), 89–186. https://www.boe.es/publicaciones/anuarios_derecho/abrir_pdf.php?id=ANU-P-199510008900186_ANUARIO_DE_DERECHO_PENAL_Y_CIENCIAS_PENALES_La_terminacion_del_delito

Calderón, F. (2021). *Construcción legislativa y aplicación jurisprudencial del delito de estafa informática en Costa Rica del año 2014 al 2019. Énfasis en el uso indebido de datos*. [Trabajo final de investigación aplicada, Universidad de Costa Rica].

Calderón, R. (2018). *El principio de legalidad: ¿Muro de contención o límite difuso para la interpretación de la teoría del delito en Costa Rica?* (2.ª ed.). Editorial Investigaciones Jurídicas S.A.

Carranza, L., & Roberto, H. (2011). *Delitos de peligro abstracto: Nuevos desafíos para la teoría del delito*. Editorial Investigaciones Jurídicas S.A.

Castillo, F. (2013). *El delito de estafa* (2.ª ed.). Editorial Jurídica Continental.

Castillo, F. (2016). *La estafa informática*. Editorial Jurídica Continental.

Castillo, F. (2020). La estafa informática de lege lata y de lege ferenda. En G. Chan, A. Rodríguez & C. A. Parma (Coords.), *Ciencias penales y derechos humanos: Homenaje al profesor Dr. Javier Llobet Rodríguez* (pp. 821–845). Editorial Jurídica Continental.

Meneses, R. & Quintana, M. (2016). Homicidios e investigación criminal en México. *Perf. Latinoam, 24* (48), 297-318. <http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0188-76532016000200297&lng=es&nrm=iso>. ISSN 0188-7653. https://doi.org/10.18504/pl2448-012-2016.

Universitat Oberta de Catalunya. (2022). Análisis Multivariante: Análisis Múltiple de Datos. Material Didáctico del curso "Matemáticas y estadística*"* 22.508 del Grado de Ciencia de Datos Aplicada. https://materials.campus.uoc.edu/continguts/PID_00221785/recursos/elmodelderegressiomultiple.pdf

Jurisprudencia

Sala Constitucional de la Corte Suprema de Justicia. Resolución N.º 1877-90 de las dieciséis horas con dos minutos del diecinueve de diciembre de mil novecientos noventa.

Sala Constitucional de la Corte Suprema de Justicia. Resolución N.º 447-91 de las quince horas con treinta minutos del veintiuno de febrero de mil novecientos noventa y uno. Sala Constitucional de la Corte Suprema de Justicia. Resolución N.º 2000-92 de las catorce horas con cero minutos del veintinueve de julio de mil novecientos noventa y dos.

Sala Constitucional de la Corte Suprema de Justicia. Resolución N.º 490-94 de las dieciséis horas con quince minutos del veinticinco de enero de mil novecientos noventa y cuatro.

Sala Constitucional de la Corte Suprema de Justicia. Resolución N.º 2000-11524 de las catorce horas con cincuenta y ocho minutos del veintiuno de diciembre de dos mil.

Sala de Casación Penal de la Corte Suprema de Justicia. Resolución N.º 00923-2002 de las nueve horas con diez minutos del veinte de septiembre de dos mil dos.

Sala de Casación Penal de la Corte Suprema de Justicia. Resolución N.º 01162-2002 de las nueve horas con tres minutos del veintidós de noviembre de dos mil dos.

Sala de Casación Penal de la Corte Suprema de Justicia. Resolución N.º 00148-2006 de las nueve horas con cero minutos del veinticuatro de febrero de dos mil seis.

Sala de Casación Penal de la Corte Suprema de Justicia. Resolución N.º 0753-07 de las quince horas con cincuenta minutos del veintitrés de julio de dos mil siete.

Sala de Casación Penal de la Corte Suprema de Justicia. Resolución N.º 01055-2009 de las ocho horas con cincuenta minutos del veintiocho de agosto de dos mil nueve.

Sala de Casación Penal de la Corte Suprema de Justicia. Resolución N.º 1076-2020 de las trece horas con veinticinco minutos del veintiocho de agosto de dos mil veinte.

Tribunal de Apelación de Sentencia Penal del Segundo Circuito Judicial de San José. Resolución N.º 587-2016 de las nueve horas con veinte minutos del veintidós de abril de dos mil dieciséis.

Tribunal de Apelación de Sentencia Penal del Segundo Circuito Judicial de San José. Resolución N.º 0617-2017 de las catorce horas con veinte minutos del veintiséis de mayo de dos mil diecisiete.

Tribunal de Apelación de Sentencia Penal del Segundo Circuito Judicial de San José. Resolución N.º 01750-2018 de las dieciséis horas con treinta minutos del tres de diciembre de dos mil dieciocho.

Tribunal de Apelación de Sentencia Penal del Segundo Circuito Judicial de San José. Resolución N.º 1899-2018 de las ocho horas con veinte minutos del veintiuno de diciembre de dos mil dieciocho.

Tribunal de Apelación de Sentencia Penal del Segundo Circuito Judicial de San José. Resolución N.º 1818-2019 de las diez horas con cinco minutos del once de octubre de dos mil diecinueve.

Tribunal de Apelación de Sentencia Penal del Segundo Circuito Judicial de San José. Resolución N.º 0494-2020 de las ocho horas con cinco minutos del veintiséis de marzo de dos mil veinte.

Tribunal de Apelación de Sentencia Penal del Segundo Circuito Judicial de San José. Resolución N.º 00349-2021 de las once horas con veinte minutos del cuatro de marzo de dos mil veintiuno.

Tribunal de Apelación de Sentencia Penal del Segundo Circuito Judicial de San José. Resolución N.º 1838-2022 de las nueve horas con quince minutos del veinte de diciembre de dos mil veintidós.

Tribunal de Apelación de Sentencia Penal del Segundo Circuito Judicial de San José. Resolución N.º 01461-2023 de las trece horas con diez minutos del treinta de octubre de dos mil veintitrés.

Páginas y Sitios Web

Asamblea Legislativa. (2009). Proyecto de ley N.º 17.613: Reforma al artículo 229 bis del Código Penal y adición de un nuevo capítulo denominado “Delitos Informáticos”. https://proyectos.conare.ac.cr/asamblea/17613%20Informe%20final.pdf

Asociación Iberoamericana de Ministerios Públicos. (s.f.). Red Iberoamericana de Fiscales Especializados en Ciberdelincuencia – CIBERRED. https://www.aiamp.info/index.php/redes-permanentes-aiamp/red-de-ciberdelincuencia

Conferencia de Ministros de Justicia de los Países Iberoamericanos. (s.f.). https://comjib.org/

Consejo de Europa. (s.f.). Convenio de Budapest sobre la Ciberdelincuencia. https://www.coe.int/en/web/cybercrime/the-budapest-convention

Consejo de Europa. (s.f.). Comité del Convenio sobre la Ciberdelincuencia. https://www.coe.int/en/web/cybercrime/tcy

Consejo de Europa. (s.f.). Comunidad de Ciberdelincuencia Octopus. https://www.coe.int/en/web/octopus/home

Consejo de Europa. (s.f.). Oficina del Programa sobre Ciberdelincuencia (C-PROC). https://www.coe.int/en/web/cybercrime/cybercrime-office-c-proc-

El Pacto. (s.f.). Europa Latinoamérica Programa de Asistencia contra el Crimen Transnacional Organizado. https://www.elpaccto.eu/

Agencia de la Unión Europea para la Cooperación Judicial Penal. (s.f.). Red Judicial Europea sobre Ciberdelincuencia. https://www.eurojust.europa.eu/crime-types-and-cases/crime-types/cybercrime

Europol. (s.f.). Centro Europeo de Ciberdelincuencia - EC3. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

Fiscalía Ministerio Público de Chile. (s.f.). Unidad Especializada en Lavado de Dinero, Delitos Económicos y Crimen Organizado. http://www.fiscaliadechile.cl/Fiscalia/quienes/fiscaliaNac_unidades_divisiones.jsp

Ministerio Fiscal. (s.f.). Fiscalía General del Estado de España: Fiscal de Sala Coordinadora en materia de Criminalidad Informática. https://www.fiscal.es/-/criminalidad-informatica

Ministerios Públicos CPLP. (s.f.). Fórum Ciberdelito y Prueba Digital de los países de la CPLP. https://www.ministeriospublicoscplp.org/redes

Ministerio Público de Portugal. (s.f.). Oficina Ciberdelito de la Procuraduría General de la República de Portugal. https://cibercrime.ministeriopublico.pt/es

Ministerio Público Fiscal de Argentina. (s.f.). Unidad Fiscal Especializada en Ciberdelincuencia. https://www.mpf.gob.ar/ufeci/

Ministerio Público Federal. (s.f.). Grupo de Apoyo en Cibercrimen – GACC. http://www.mpf.mp.br/atuacao-tematica/ccr2/coordenacao/comissoes-e-grupos-de-trabalho/combate-crimes-cirberneticos/sobre

Oficina de las Naciones Unidas contra la Droga y el Delito. (s.f.). Programa Global sobre Ciberdelincuencia. https://www.unodc.org/unodc/es/cybercrime/global-programme-cybercrime.html

Organización de Estados Americanos. (s.f.). Portal Interamericano de Cooperación en Delito Cibernético. http://www.oas.org/es/sla/dlc/cyber-es/homePortal.asp

Peña, T. (2023, 26 de junio). Análisis semanal 501: El cibercrimen y su conexión con el crimen organizado.

Observatorio de la Política Internacional. https://opi.ucr.ac.cr/node/1974

Unión Europea. (s.f.). Portal de la Unión Europea sobre ciberdelito. https://ec.europa.eu/home-affairs/cybercrime_en

Oficina de las Naciones Unidas contra la Droga y el Delito. (2019). Ciberdelincuencia organizada: Grupos criminales involucrados. https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/criminal-groups-engaging-in-cyber-organized-crime.html

Oficina de las Naciones Unidas contra la Droga y el Delito. (2019). Ciberdelincuencia organizada: ¿Qué es? https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime_what-is-it.html

ANEXO 1. Base de datos de expedientes analizados empíricamente.

Este archivo contiene la recopilación sistemática de cien causas penales tramitadas por el delito de Estafa informática en el I Circuito Judicial de Alajuela en los años 2020 a 2023, en la etapa preparatoria e intermedia; analizadas a efectos de determinar su tratamiento judicial.

NUE	¿OIJ realizó Actos de investigación?	Valor X1	¿MP solicitó a Juzg Penal actos de investigación?	Valor X2	¿Acto Conclusivo Ministerio Público?	Valor X3	Fundamento Ministerio Público	Valor X4	Acto Conclusivo JP	Valor x5	¿Delito impune?	Y
20-002056-0057-PE	SI	1	NO	0	Solicitud Desestimación	1	Atipicidad	1	Desestimación	1	SI	1
20-002095-0057-PE	SI	1	NO	0	Solicitud Desestimación	1	Falta de elementos probatorios	2	Desestimación	1	SI	1
20-001228-0062-PE	SI	1	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	1	SI	1
20-001255-0069-PE	SI	1	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	1	SI	1
20-001517-0068-pe	SI	1	SI	1	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	1	SI	1
20-001003-0057-PE	NO	0	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	1	SI	1
20-000925-0057-PE	NO	0	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	1	SI	1
20-001060-0057-PE	SI	1	NO	0	Solicitud Sobreseimiento Definitivo	3	Desinterés víctima	3	Sobreseimiento Definitivo	2	SI	1
20-000993-0075-PE	SI	1	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	1	SI	1
20-000843-0075-PE	SI	1	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	1	SI	1
20-000830-0799-PE	SI	1	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	1	SI	1
20-000899-0057-PE	SI	1	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	1	SI	1
20-000316-0057-PE	SI	1	NO	0	Criterio de oportunidad	4	Criterio de Oportunidad	4	Sobreseimiento Definitivo	2	SI	1
20-000105-0989-PE	SI	1	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	1	SI	1
20-000417-0057-PE	SI	1	NO	0	Solicitud Desestimación	1	Falta de elementos probatorios	2	Desestimación	1	SI	1
20-000416-0067-PE	SI	1	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	1	SI	1
20-000591-0057-PE	SI	1	SI	1	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	1	SI	1
20-000517-0057-PE	SI	1	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	1	SI	1
20-000511-0074-PE	SI	1	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	1	SI	1
20-000586-0057-PE	NO	0	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	1	SI	1
20-000580-0071-PE	SI	1	SI	1	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	1	SI	1
20-000592-0057-PE	NO	0	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	1	SI	1
20-000701-0057-PE	NO	0	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	1	SI	1
20-000725-0057-PE	SI	1	SI	1	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	1	SI	1
20-000749-0057-PE	SI	1	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	1	SI	1
20-000718-0057-PE	SI	1	NO	0	Solicitud Desestimación	1	Falta de elementos probatorios	2	Desestimación	1	SI	1
20-001998-0057-PE	SI	0	NO	0	Solicitud Desestimación (#1) / Criterio de Oportunidad (#2)	2	Desinterés víctima / Criterio de Oportunidad	3	Sobreseimiento Definitivo	2	SI	1
20-000318-0057-PE	SI	1	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	0	SI	1
20-000001-1310-CC	SI	1	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	0	SI	1
20-000194-0832-PE	SI	1	SI	1	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	0	SI	1
20-002051-0057-PE	SI	1	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	0	SI	1
20-002139-0057-PE	SI	1	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	0	SI	1
20-002112-0057-PE	SI	1	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	0	SI	1
20-001468-0057-PE	SI	1	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	0	SI	1
20-001399-0067-PE	SI	1	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	0	SI	1
20-001347-0305-PE	SI	1	SI*	0	Solicitud Desestimación	1	Falta de elementos probatorios	2	Desestimación	0	SI	1
17-016075-0042-PE	SI	1	SI	1	Solicitud Sobreseimiento Definitivo	3	Falta de elementos probatorios	2	Actividad Procesal Defectuosa	3	NO	0

NUE	¿OIJ realizó Actos de investigación?	Valor X1	¿MP solicitó a Juzg Penal actos de investigación?	Valor X2	¿Acto Conclusivo Ministerio Público?	Valor X3	Fundamento Ministerio Público	Valor X4	Acto Conclusivo JP	Valor x5	¿Delito impune?	Y
20-002315-0057-PE*	SI	1	NO	0	Solicitud Sobreseimiento Definitivo	3	Prescripción	6	Sobreseimiento Definitivo	2	SI	1
20-002076-0068-PE	SI	1	NO	0	Solicitud Desestimación	1	Falta de elementos probatorios	2	Desestimación	0	SI	1
20-001944-0057-PE	SI	1	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	0	SI	1
20-001986-0057-PE	SI	1	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	0	SI	1
20-001881-0057-PE	SI	1	SI	1	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	0	SI	1
20-001929-0057-PE	SI	1	SI	1	Solicitud Desestimación	1	Falta de elementos probatorios	2	Desestimación	0	SI	1
20-004721-0057-PE	SI	1	SI	1	Solicitud Desestimación (#1) / Criterio de Oportunidad (#2)	2	Criterio de Oportunidad	4	Sobreseimiento Definitivo	2	SI	1
20-000178-0057-PE	SI	1	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	0	SI	1
20-000090-0057-PE	SI	1	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	0	SI	1
20-000365-1093-PE	SI	1	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	0	SI	1
20-002221-0058-PE	SI	1	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	0	SI	1
20-001341-0057-PE	SI	1	SI	1	Solicitud Desestimación	1	Falta de elementos probatorios	2	Desestimación	0	SI	1
20-002019-0058-PE	SI	1	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	0	SI	1
20-001936-0057-PE	SI	1	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	0	SI	1
20-001960-0057-PE	SI	1	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	0	SI	1
20-001932-0068-PE	SI	1	SI	1	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	0	SI	1
20-001956-0042-PE	SI	1	NO	0	Solicitud Sobreseimiento Definitivo	3	311 INCISO E	7	Sobreseimiento Definitivo	2	SI	1
20-001944-0057-PE	SI	1	SI	1	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	0	SI	1
20-001823-0057-PE	SI	1	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	0	SI	1
22-000274-0068-PE	SI	1	SI	1	Solicitud Sobreseimiento Definitivo	3	Criterio de Oportunidad	4	Sobreseimiento Definitivo	2	SI	1
18-000683-0057-PE	SI	1	SI	1	Solicitud Sobreseimiento Definitivo	3	Falta de elementos probatorios	2	Disconformidad	5	NO	0
18-000977-0057-PE	SI	1	NO	0	Solicitud Sobreseimiento Definitivo	3	Falta de elementos probatorios	2	Actividad Procesal Defectuosa	3	NO	0
19-001979-057-PE	SI	1	SI	1	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	0	SI	1
19-003247-0057-PE	SI	1	SI	1	Solicitud Desestimación	1	Falta de elementos probatorios	2	Disconformidad	5	NO	0
19-004219-0059-PE	SI	1	SI	1	Solicitud Desestimación	1	Falta de elementos probatorios	2	Actividad Procesal Defectuosa	3	NO	0
19-004406-0057-PE	SI	1	SI	1	Solicitud Desestimación	1	Falta de elementos probatorios	2	Actividad Procesal Defectuosa	3	NO	0
21-000013-1104-PE	SI	1	NO	0	Solicitud Desestimación	1	Falta de elementos probatorios	2	Actividad Procesal Defectuosa	3	NO	0
17-003024-0057-PE	SI	1	SI	1	APERTURA A JUICIO	5	AUTO APERTURA A JUICIO	0	AUTO APERTURA A JUICIO	0	NO	0
20-005704-0057-PE	SI	1	SI	1	Solicitud Desestimación	1	Falta de elementos probatorios	2	Actividad Procesal Defectuosa	3	NO	0
17-001847-0057-PE	SI	1	SI	1	APERTURA A JUICIO	5	Falta de elementos probatorios	2	SuspenSión del Procedimiento a Prueba	4	NO	0
22-005705-0057-PE	SI	1	NO	0	Solicitud Desestimación	1	Falta de elementos probatorios	2	Actividad Procesal Defectuosa	3	NO	0
20-003919-0057-PE	SI	1	SI	1	Solicitud Desestimación	1	Falta de elementos probatorios	2	Actividad Procesal Defectuosa	3	NO	0
22-002483-0057-PE	SI	1	NO	0	Solicitud Desestimación	1	Falta de elementos probatorios	2	Actividad Procesal Defectuosa	3	NO	0

NUE	¿OIJ realizó Actos de investigación?	Valor X1	¿MP solicitó a Juzg Penal actos de investigación?	Valor X2	¿Acto Conclusivo Ministerio Público?	Valor X3	Fundamento Ministerio Público	Valor X4	Acto Conclusivo JP	Valor x5	¿Delito impune?	Y
19-023965-0042-PE	SI	1	NO	0	Solicitud Sobreseimiento Definitivo	3	Prescripción	6	Actividad Procesal Defectuosa	3	NO	0
22-000151-0829-PE	SI	1	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Actividad Procesal Defectuosa	3	NO	0
21-003968-0057-PE	SI	1	SI	1	Solicitud Sobreseimiento Definitivo	3	311 INCISO E	7	Actividad Procesal Defectuosa	3	NO	0
21-002590-0057-PE	SI	1	SI	1	Solicitud Desestimación	1	Falta de elementos probatorios	2	Actividad Procesal Defectuosa	3	NO	0
22-007849-0059-PE	SI	1	NO	0	Solicitud Desestimación	1	Falta de elementos probatorios	2	Actividad Procesal Defectuosa	3	NO	0
22-004265-0057-PE	SI	1	NO	0	Solicitud Desestimación	1	Falta de elementos probatorios	2	Actividad Procesal Defectuosa	3	NO	0
21-004599-0057-PE	SI	1	NO	0	Solicitud Desestimación	1	Falta de elementos probatorios	2	Actividad Procesal Defectuosa	3	NO	0
22-002406-0057-PE	SI	1	NO	0	Solicitud Desestimación	1	Falta de elementos probatorios	2	Actividad Procesal Defectuosa	3	NO	0
21-001309-0070-PE	SI	1	NO	0	Solicitud Desestimación	1	Falta de elementos probatorios	2	Actividad Procesal Defectuosa	3	NO	0
22-000216-0799-PE	SI	1	NO	0	Solicitud Desestimación	1	Falta de elementos probatorios	2	Actividad Procesal Defectuosa	3	NO	0
22-000224-0074-PE	SI	1	SI	1	Solicitud Sobreseimiento Definitivo	3	Criterio de Oportunidad	4	Sobreseimiento Definitivo	2	SI	1
22-000244-0065-PE	SI	1	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	0	SI	1
20-001753-0057-PE	SI	0	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	0	SI	1
20-001794-0057-PE	SI	0	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	0	SI	1
20-001727-0057-PE	SI	1	NO	0	Solicitud Desestimación	1	Falta de elementos probatorios	2	Desestimación	0	SI	1
20-001645-0057-PE	SI	1	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	0	SI	1
20-001838-0057-PE	SI	1	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	0	SI	1
20-001820-0059-PE	SI	1	NO	0	Solicitud Sobreseimiento Definitivo	3	Criterio de Oportunidad	4	Sobreseimiento Definitivo	2	SI	1
20-000293-0057-PE	SI	1	SI	1	Solicitud Sobreseimiento Definitivo	3	Criterio de Oportunidad	4	Actividad Procesal Defectuosa	3	NO	0
20-000055-0057-PE	SI	1	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	0	SI	1
20-001110-0057-PE	SI	1	SI	1	Solicitud Sobreseimiento Definitivo	3	Criterio de Oportunidad	4	Actividad Procesal Defectuosa	3	NO	0
20-001137-0042PE	SI	1	SI	1	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	0	SI	1
20-001896-0060-PE	SI	1	SI	1	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	0	SI	1
20-001844-0057-PE	SI	1	SI	1	Solicitud Desestimación	1	Falta de elementos probatorios	2	Desestimación	0	SI	1
20-001867-0057-PE	SI	1	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	0	SI	1
20-001154-0060-PE	SI	1	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	0	SI	1
22-000547-0058-PE	SI	1	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	0	SI	1
22-000031-0059-PE	SI	1	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	0	SI	1
21-003956-0057-PE	SI	1	NO	0	Solicitud Desestimación	1	Desinterés víctima	3	Desestimación	0	SI	1
17-003891-0057-PE	SI	1	SI	1	APERTURA A JUICIO	5	AUTO APERTURA A JUICIO	0	AUTO APERTURA A JUICIO	0	NO	0

SI = 1

NO = 0

			Atipicidad	1	
			Falta de elementos probatorios	2	Desestimación 1
			Desinterés víctima	3	Sobreseimiento Definitivo 2
	Solicitud Desestimación	1	Criterio de Oportunidad	4	Actividad Procesal Defectuosa 3

Solicitud Desestimación (#1) / Criterio de Oportunidad (#2)	2	Desinterés víctima / Criterio de Oportunidad	3	SuspenSIón del Procedimiento a Prueba	4
Solicitud Sobreseimiento Definitivo	3	Prescripción	6	Disconformidad	5
Criterio de oportunidad	4	311 inciso E	7		
APERTURA A JUICIO	5			AUTO APERTURA A JUICIO	0