FACULTAD DE DERECHO

Responsabilidad del ciberburrier en el delito de fraude informático

Tesis para optar el Título de

Abogado

Mario Ramiro De Valdivia Lozada

Asesor(es):
Dr. Eduardo Arsenio Oré Sosa

Lima, octubre de 2023

UNIVERSIDAD DE PIURA

Declaración Jurada de Originalidad del Trabajo Final

Yo, Mario Ramiro De Valdivia Lozada, egresado(a) del Programa Académico de Derecho, de la Facultad de Derecho de la Universidad de Piura, identificado(a) con DNI 70322175

Declaro bajo juramento que:

1. Soy autor del trabajo final titulado:
   "Responsabilidad del *ciberburrier* en el delito de fraude informático "
   El mismo que presento bajo la modalidad de tesis[1] para optar el Título Profesional[2] de Abogado

2. La asesoría del trabajo está a cargo de:
   - **Eduardo Arsenio Oré Sosa.**, identificado con DNI N° 10293037
3. El texto de mi trabajo final respeta y no vulnera los derechos de terceros, o de ser el caso derechos de los coautores, incluidos los derechos de propiedad intelectual, datos personales, entre otros. En tal sentido, el texto de mi trabajo final no ha sido plagiado total ni parcialmente, para la cual he respetado las normas internacionales de citas y referencias de las fuentes consultadas.
4. El texto del trabajo final que presento no ha sido publicado ni presentado antes en cualquier medio físico o electrónico.
5. La investigación, los resultados, datos, conclusiones y demás información presentada que atribuyo a mi autoría son veraces.
6. Declaro que mi trabajo final cumple con todas las normas de la Universidad de Piura.

El incumplimiento de lo declarado da lugar a responsabilidad del declarante, en consecuencia; a través del presente documento asumo frente a terceros, la Universidad de Piura y/o la Administración Pública toda responsabilidad que pueda derivarse por el trabajo final presentado. Lo señalado incluye responsabilidad pecuniaria incluido el pago de multas u otros por los daños y perjuicios que se ocasionen.

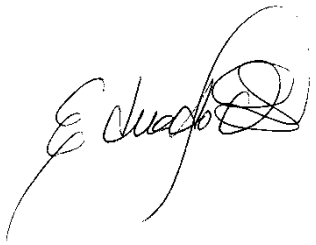
Fecha: 23 de octubre de 2023

Firma del optante[3]

[1] Indicar si es tesis, trabajo de investigación, trabajo académico o trabajo de suficiencia profesional.
[2] Grado de Bachiller, Título de profesional, Grado de Maestro o Grado de Doctor
[3] Idéntica a DNI, no se admite digital salvo certificado

Aprobación

Tesis titulada “Responsabilidad del *ciberburrier* en el delito de fraude informático”, presentada por el bachiller Mario Ramiro De Valdivia Lozada, en cumplimiento con los requisitos para obtener el Título de Abogado. Fue aprobada por el Director de Tesis, Doctor Eduardo Arsenio Oré Sosa.



Eduardo Arsenio Oré Sosa
Director de Tesis

Resumen

El objeto del presente trabajo será analizar la institución jurídica del "*ciberburrier*" en la comisión del delito de fraude informático. Organizaciones o individuos que planifican este ilícito contactan al *ciberburrier* para solicitarle recibir transferencias bancarias y remitir posteriormente el dinero a determinadas cuentas bancarias, a cambio del pago de una comisión. La pregunta que el presente trabajo busca responder es si estos *ciberburriers* pueden responder como cómplices de fraude informático o como autores de algún otro delito; en particular, de receptación o de lavado de activos. En muchos casos, surgen dudas sobre si los *ciberburriers* realmente conocían la procedencia del dinero, o sospechaban de la comisión de algún ilícito penal. No es infrecuente que sujetos que no tienen ninguna relación con defraudadores vean que sus cuentas bancarias han sido signadas como cuentas de destino para los fondos objeto de fraude. Así, reciben un dinero de origen desconocido, y luego son contactados por sujetos que, sin necesariamente revelar dicho origen, les solicitan la transferencia de los activos, indicando, generalmente, que el depósito se debe a un equívoco. Esta modalidad delictiva hace necesaria la investigación penal, a fin de determinar el grado de participación y/o de autoría de estos intermediarios. Este trabajo engloba tres capítulos:

El primer capítulo introduce el marco legislativo general en el que se encuadra los delitos informáticos. En particular, se explora, por un lado, el Convenio de Budapest sobre la Ciberdelincuencia (2001) y otras iniciativas internacionales en la lucha contra la criminalidad informática, y, por otro, la legislación penal acogida por el Perú en materia de juzgamiento de fraude informático. El segundo capítulo gira en torno al delito de fraude informático en el Perú, el cual constituye el objeto principal bajo estudio. Se realiza un análisis del tipo penal y se articulan la tipicidad objetiva y la subjetiva, con miras a dilucidar en qué consiste la comisión de este ilícito penal. El capítulo concluye con un breve análisis de cuestiones probatorias y procesales que suelen ser relevantes en el juzgamiento de este delito. El tercer capítulo aborda el problema fundamental de determinar la responsabilidad penal del *ciberburrier*. A grandes rasgos, se considerará tres posibilidades. La primera de ellas consiste en la posibilidad de que el *ciberburrier* responda como partícipe del delito de fraude informático. Las dos posibilidades siguientes consisten en la imputación, en calidad de autor, de los delitos de receptación y lavado de activos. Luego de analizar estas tres posibilidades, y la subsiguiente posibilidad de encontrarnos ante un concurso de delitos, el capítulo concluye con una toma de posición con respecto a la manera idónea de determinar la responsabilidad penal del *ciberburrier*.

Tabla de contenido

Introducción

En la actualidad, los avances en las tecnologías de la información y la comunicación (TIC) y, en particular, la internet, han permitido enormes progresos en la comunicación a nivel global, incluyendo al Perú, brindando grandes oportunidades de desarrollo individual y social, posibilitando conexiones a nivel mundial, eliminando las distancias en la intercomunicación entre las personas, pues en este contexto las TIC traen consigo tanto beneficios como desventajas, ya que los usuarios al servirse de los medios tecnológicos de forma ilícita, generan para sí beneficios y ocasionan perjuicios a terceros, siendo consideradas estas conductas como negativas y denominadas conductas delictivas en el ámbito jurídico, porque provocan riesgos a bienes jurídicos tales como la intimidad personal, la privacidad, la seguridad, y la propiedad.

En efecto, en el Perú todos los ciudadanos podemos verificar la alarmante crisis respecto del incremento de la delincuencia cibernética. Así, el Estado peruano tiene el rol básico de establecer y garantizar el bienestar social respecto del uso de sistemas informáticos. En ese contexto, surge la División de Investigación de Delitos de Alta Tecnología- DIVINDAT, dependencia de la Policía Nacional del Perú que brinda un gran aporte respecto de la investigación mediante la recopilación de información del hecho delictivo y la elaboración de estadísticas del incremento de la delincuencia cibernética.

Asimismo, en el marco jurídico peruano, se han venido desarrollando herramientas materiales y procesales derivadas de la adhesión del Perú al Convenio de Cibercriminalidad, también conocido como Convenio de Budapest, tratado multilateral que delimita las particularidades de los delitos informáticos y las medidas que deben adoptarse frente a los mismos a nivel nacional mediante la cooperación entre Estados, así sucede, por ejemplo, con la promulgación de la Ley N° 30096, Ley de delitos informáticos y su modificatoria, la Ley N° 30171, las cuales han seguido los parámetros del Convenio. Por lo tanto, en el presente trabajo el objetivo es revisar y analizar el marco jurídico vigente referido al fraude informático; en específico, determinar si la conducta ilícita realizada por el *ciberburrier* se encuentra inmersa dentro del fraude informático, receptación o lavado de activos.

Esta tesis está estructurada en tres capítulos. El primero presenta los antecedentes de los delitos informáticos, en concordancia al Convenio de Budapest y la cooperación internacional, la cual facilita la obtención de información, la persecución y la represión del delito, luchando contra la criminalidad informática; así como los antecedentes de la legislación penal acogida por el Perú en materia de delitos informáticos.

El segundo capítulo gira en torno al delito de fraude informático en el Perú, analizando la figura jurídica antes mencionada, el tipo penal, la tipicidad objetiva y subjetiva, con la finalidad de aclarar en qué consiste la comisión de este ilícito penal. El capítulo concluye con un breve análisis de los aspectos procesales y medios probatorios digitales en la comisión de este delito.

El tercer capítulo aborda el problema fundamental de determinar la responsabilidad penal del *ciberburrier*. A grandes rasgos, se considerarán tres posibilidades. La primera de ellas consiste en la posibilidad de que el *ciberburrier* responda como partícipe del delito de fraude informático. Las dos posibilidades siguientes consisten en la imputación en calidad de autor de los delitos de receptación y de lavado de activos, respectivamente. Además, se analizará la posibilidad de un concurso de delitos. Luego de analizar estas posibilidades, el capítulo concluye con una toma de posición personal respecto a la manera idónea de determinar la responsabilidad penal del *ciberburrier*.

Capítulo I: Delitos informáticos

En este capítulo delimitaremos el inicio de los delitos informáticos, los cuales se encuentran tipificados en el marco normativo nacional e internacional. Además, indagaremos las acciones que el Estado peruano ha tomado contra estos delitos.

1.1. Antecedentes

En palabras de Moisés Barros, las tecnologías de la información y la comunicación (TIC) son "(...) grandes paradigmas que experimentan la tecnología en información, y que ha aumentado de una u otra manera la forma en que las personas se comunican puesto que para enviar cualquier tipo de información o mensaje se requiere de alguna vía o canal para que este pueda circular".[4]

En particular, la Internet ofrece un beneficio de manera significativa siempre que sea utilizado de forma correcta, ya que permite que cualquier persona pueda estar conectada mediante un dispositivo tecnológico con conexión a red; es decir, la Internet tiene un carácter abierto, transparente y descentralizado, lo cual constituye el pilar fundamental para la configuración de partes esenciales de la Internet a través de su uso final.[5]

En ese sentido, las TIC han permitido cuantiosos beneficios, como la creación de aparatos tecnológicos; por ejemplo, las computadoras, cuyas "(…) posibilidades (…) son inmensas, infinitas; permiten una verdadera enseñanza conforme a las ideas, las necesidades y lo que pretende el hombre, llegando a hacer muchas cosas como esta, pero a mucha velocidad y sin cansancio."[6] Sin embargo, el surgimiento de las TIC también implica riesgos e impactos negativos, como la aparición de delitos informáticos, que son comportamientos ilícitos realizados a través del uso de la tecnología y la conectividad, sin limitación de fronteras físicas.

Es así que nos remontamos a la época de los sesentas, década en la que se dio inicio a la revolución cibernética. El uso de la computadora generó una revolución en la obtención de la información, gatillando un nuevo sistema de comunicaciones y provocando, a su vez, lamentablemente, la comisión de ilícitos. No obstante, como dato histórico, podemos afirmar

---

[4] Oscar Barros, *Tecnologías de la información y su uso en gestión* (Chile: McGraw Hill, 1998), 20.

[5] Lester Lessig Lawrence, *El Código y otras leyes del ciberespacio* (Madrid: Grupo Santillana, 2001), 21.

[6] Julio Nuñez Ponce, "Apuntes sobre la protección jurídica del Software o programas de computadoras", *Ius Et Praxis*, 007, (1986): 129 https://doi.org/10.26439/iusetpraxis1986.n007.3337.

que los delitos informáticos no eran considerados ilícitos penales en esta época, ya que la postura tradicional de la década en mención aún no regulaba penalmente los asuntos informáticos.

Por ejemplo, uno de los delitos más comunes en aquella época era el llamado "fraude telefónico", referido al uso no habitual de medios de comunicación masiva , generándose de esta manera, por ejemplo, el uso gratuito del servicio telefónico o "cajas azules", como eran conocidas popularmente.[7] Estos objetos emitían un sonido especial reconocido por las computadoras, con la finalidad de que los individuos obtengan acceso ilegítimo a servicios de llamada a larga distancia, sin pagar su coste, lo que en esa época se consideraba fraude telefónico.

Así como la conducta antes descrita, surgieron progresivamente varios tipos de ilícitos penales, conforme al rápido avance de la tecnología; en mérito a esta situación, apareció la necesidad de crear sistemas de protección de la información y datos personales, sobre todo ante la amenaza de los novedosos virus informáticos, los cuales eran implantados en las computadoras, ingresando a las bases de datos financieros y logrando llevar a cabo ataques cibernéticos.

Es en los años 80 que se expanden masivamente los ataques a través de virus informáticos. Ello provocó el incremento de la práctica de fraudes, espionajes informáticos, hacking y piraterías de software[8], generando vacíos legales, pues los comportamientos ilícitos no se encontraban tipificados en la norma y, a raíz de esta situación, surge la imperiosa necesidad de salvaguardar y proteger los derechos vulnerados de las personas, exigiendo una innovación en el marco jurídico respecto de los delitos informáticos.

Como consecuencia de todo lo mencionado, la Organización de Cooperación y Desarrollo Económico (OCDE) tuvo la iniciativa de elaborar un conjunto de normas penales que tenían por objetivo combatir el uso delictivo de programas informáticos mediante las computadoras, siendo el primer intento de regulación sobre la materia.

Continuando en orden cronológico, en la década de los 90, el uso del internet se encontraba altamente masificado y surgió así una nueva modalidad de delito informático: la proliferación de virus encriptados, vinculados a la publicidad que se mostraban en las diferentes páginas web a las que los usuarios accedían. Al ingresar a estas páginas con exceso de

[7] Álvaro, Burgos Mata, "El Delito Informático," Acta *Académica*. Núm. 47 (2010): 177-179.
[8] Julio, Mazuelos Coello, "Modelos de imputación en el Derecho penal informático," *Derecho Penal y criminología*, 28, núm. 85 (2007): 39.

publicidad, que contenían virus encriptados, se afectó directamente al comercio electrónico y al desarrollo de las operaciones económicas que se realizaban por este medio.

Simultáneamente, empezaron a aparecer páginas que vulneraban la intimidad y privacidad de las personas, difundiendo contenido íntimo y otros basados en el abuso sexual a menores de edad. Todo ello alarmó a las autoridades tanto nacionales e internacionales, como por ejemplo la Asociación Internacional de Derecho Penal, la cual emitió un documento durante el coloquio celebrado en Wurzburgo en 1992, adoptando diversas recomendaciones respecto de la tipificación de todos los comportamientos ilícitos en mención y en torno al cambio normativo que debía darse a nivel estatal con el fin de combatir estas nuevas formas de criminalidad. Resulta trascendente mencionar que, en el marco de dicho evento, se debatió sobre si estos nuevos delitos debían ser considerados delitos informáticos o ingresarían en la línea de los delitos tradicionales.

Es así que, países como Estados Unidos, Francia, el Reino Unido, Países Bajos, Chile, Austria, Italia, Portugal, España, Venezuela, Argentina y México realizaron cambios en sus respectivas normativas, combinando leyes especiales y agregando artículos a sus respectivos Códigos Penales referidos a delitos informáticos.[9]

Ya en este siglo, a inicios del año 2000, con el advenimiento de las redes sociales, se produjo un significativo incremento de las bases de datos de información personal, lo que, naturalmente, trajo como consecuencia la comisión de delitos respecto de su uso indebido, surgiendo así negocios muy lucrativos, cuyo objetivo reside en obtener la información personal de los usuarios (familiares, intereses, gustos, entre otros datos de relevancia), a efectos de utilizarla con fines comerciales.

En lo que respecta al Perú, anteriormente el Código Penal, en su artículo 183, inciso 3, segundo párrafo, regulaba los delitos informáticos sólo como un agravante del delito de hurto, mas no como un delito autónomo.[10] Posteriormente, el 17 de julio del 2000, entró en vigor la Ley N° 27309, la cual modificó el Título V, del Libro Segundo del Código Penal, e incorporó el Capítulo X, llamado Delitos Informáticos, en el que se introdujeron los siguientes delitos:

- Intrusismo y fraude informático (Art. 207-A),
- Sabotaje informático (Art. 207-B),
- Circunstancias agravantes (Art. 207-C) y

[9] Eduardo Urbano Castrillo, *Delincuencia Informática, Tiempos de cautela y amparo*, (Pamplona: Thomson Reuters, Aranzadi, 2012) 45-58.
[10] Luis Bramont – Arias, "Delitos informáticos", *Revista Peruana de Derecho de la Empresa, Derecho informático Y Teleinformática Jurídica,* núm. 51 (2000)*:* 85 – 91.

- Tráfico ilegal de datos (Art. 207-D).

Con la dación de la Ley N° 27309, se buscaba proteger al patrimonio, por ser considerado el bien jurídico amenazado en los delitos informáticos; sin embargo, con el devenir tecnológico podemos observar que los ilícitos penales informáticos no sólo afectan al patrimonio, sino que vulneran los derechos a la intimidad, la privacidad, propiedad intelectual, así como la transgresión de la protección de la información personal, entre otros. Por lo tanto, como podemos apreciar, la nueva normativa presentaba deficiencias.[11]

Luego, en el año 2013 se aprobó por unanimidad la Ley N° 30096, Ley de Delitos informáticos, publicada el 22 de octubre del 2013 en el Diario Oficial El Peruano, la cual tenía como finalidad sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información.

Para finalizar este punto, es necesario destacar la influencia del antes mencionado Convenio de Budapest, tratado que fue incorporándose en legislaciones nacionales y el Perú no fue una excepción, pues evaluó adherirse a él con el objeto de introducir cambios en la legislación penal en relación a los delitos informáticos. En consecuencia, el 10 de marzo del 2014 se publicó la Ley N° 30171, la cual modificó la Ley N°30096, a fin de adecuar los lineamientos jurídicos nacionales a los fijados en el Convenio de Budapest.

1.2. El Convenio de Cibercriminalidad y la cooperación internacional contra la criminalidad informática

1.2.1. El Convenio de Budapest

1.2.1.1. Antecedentes del Convenio de Budapest. El Consejo de Europa tiene como objetivo lograr la unión y cooperación de los Estados que lo conforman, con el fin de mantener el equilibrio entre los intereses de la acción penal y el respeto de los derechos humanos fundamentales.

En el año 1996, a fin de formalizar las sugerencias brindadas por el Consejo en el año 1989, referidas a la necesidad de la acción penal en base a las conductas ilícitas por medio de la internet, se instaura un comité en Europa, denominado Comité de expertos encargados de delitos informáticos, mediante documento número CDPC/103/211196. El mencionado comité

[11] Hugo Vizcardo y Jorge Silfredo, "Tipificación De Los Delitos Informáticos Patrimoniales En La Nueva Ley De Delitos Informáticos N° 30096" *Alma Mater* 1, núm.1 (2014):77.

tenía el objetivo de analizar las recomendaciones de procedimiento penal y elaborar un borrador de una norma de carácter vinculante.

En el año 1997, el Consejo de Europa, mediante documento número CM/Del/Dec(97)583, conformó el Comité de expertos en la delincuencia en el ciberespacio, con la finalidad de elaborar instrumentos jurídicamente vinculantes, los cuales tengan alcance mundial y, de esta manera, facilitar la cooperación entre Estados en la exposición y persecución de los sujetos que cometen delitos por medios electrónicos.

En abril del año 2000 se publicó el proyecto del Convenio y en junio del año 2001, mediante la Sesión Plenaria N° 50 del Comité Europeo para los Problemas Criminales (CDPC), se aprobó el proyecto en mención. Finalmente, en la sesión 109 del Consejo de Europa de noviembre de 2001, se aprobó el Tratado Nº 185 del Consejo de Europa que contenía el Convenio de Budapest sobre la Ciberdelincuencia, el cual quedó expedito para ser firmado por los Estados que participaron en su formulación.

El tratado entró en vigor a nivel internacional el 1 de julio de 2004 y es considerado por la comunidad internacional como el instrumento jurídico internacional que instaura los parámetros básicos respecto de los delitos informáticos, con la meta de armonizar las legislaciones de los Estados adheridos al Convenio y el texto del tratado.

1.2.1.2. Objetivos y beneficios del Convenio de Budapest. El Convenio es uno de los primeros tratados sobre delitos cometidos a través de internet y otras redes informáticas que brinda herramientas de derecho y cooperación judicial a los Estados parte para la protección de sus ciudadanos frente a los ciberdelitos. Tiene cuarenta y ocho artículos distribuidos en cuatro capítulos; el primer capítulo contiene la terminología del convenio; el segundo desarrolla las medidas a adoptarse tanto en el derecho sustantivo y procesal; el tercero desarrolla lineamientos de cooperación entre Estados para identificar y sancionar los ciberdelitos; y el cuarto versa sobre las formalidades de adhesión de Estados y entrada en vigor del tratado.[12]

Uno de los principales objetivos del convenio es generar una política penal común y unificada, y fomentar regulaciones sobre la materia en las legislaciones de cada Estado, lo que permitiría cerrar las brechas jurídico-tecnológicas, ya que los vacíos normativos son considerados como un problema latente, sobre todo en los países subdesarrollados, los cuales devienen en paraísos cibernéticos.[13]

---

[12] Consulado de Europa, *Convenio Sobre la Ciberdelincuencia* (Budapest: Serie de Tratados Europeos Nº 185, 2001). 1-26.

[13] Suman Naresh, *Sociedad de la Información: los nuevos pobres* (Quark: Ciencia, medicina, comunicación y cultura, Nº 17, 1999) 50-51.

A continuación, los objetivos formales del Convenio de Budapest:

1. Producir un marco normativo común de derecho penal, con la meta de implantarla para proteger a los ciudadanos del cibercrimen.
2. Estandarizar los procedimientos procesales penales, consiguiendo así una legislación con base procedimental específica.
3. Promover la cooperación mundial, con el objetivo que más países se adhieran al Convenio de Budapest y se luche conjuntamente contra el flagelo del cibercrimen.

Por otra parte, cabe especificar 3 beneficios del Convenio de Budapest: el tratado no sustituye la legislación nacional, sino que mantiene la jurisdicción propia de cada Estado; es decir, cada Estado tiene autonomía en la implementación de sus normativas. Lo estipulado en el Convenio no es autoaplicativo, sino que es una referencia para que el Estado parte regule autónomamente su marco normativo.

Asimismo, otro beneficio se aprecia en los cambios procesales penales, como por ejemplo en el plazo de obtención de datos de los delitos informáticos en tiempo real, lo cual genera la conservación del valor de la prueba y que esta pueda ser utilizada dentro de un determinado proceso penal. Análogamente, el registro, confiscación y conservación de datos almacenados, casos en los que el Estado parte adoptará medidas legislativas con la finalidad de permitir una conservación óptima de datos electrónicos específicos.[14]

El tercer beneficio es la asistencia legal mutua, la cual busca la colaboración entre los Estados parte en la persecución del ciberdelito; por ejemplo, una figura contemplada por el tratado es la extradición por delitos informáticos, teniendo como requisito que el ilícito se encuentre tipificado en las legislaciones de los Estados inmersos en la extradición que se trate.[15]

1.2.2. La cooperación internacional contra la criminalidad informática

La cooperación jurídica internacional es un mecanismo por el cual los Estados se brindan colaboración en los diferentes aspectos que se presentan en un determinado proceso judicial.[16] Aplicado al presente trabajo, la cooperación jurídica internacional tiene como finalidad el apoyo entre Estados parte del convenio en la lucha contra la criminalidad informática.

---

[14] Carmen Figueroa Vavarro, "El aseguramiento de las pruebas y la cadena de custodia", *La Ley Penal*, núm 84 (2011): 4.

[15] Jesús Tirado Estrada, "Cooperación Judicial internacional en el ámbito iberoamericano. Balance y Perspectivas. Especial referencia a los procesos de instauración de medidas estructurales de relación, organización y coordinación," *Mecanismos de Cooperación Judicial Internacional* (2014): 146-150.

[16] María Luisa Montenegro,"Cooperación Internacional: Tramitación, obtención de pruebas, e incorporación de pruebas y evidencias", *Revista Jurídica Ministerio Público*, N°70 (2017): 64 – 67.

El Convenio de Budapest, desde luego, no se opone al desarrollo de las TIC, sino que busca que las mencionadas tecnologías generen progreso respetando los derechos de los ciudadanos. Por este motivo, el Convenio busca reformular la legislación en protección de los usuarios de las tecnologías en el ámbito nacional y de esta manera armonizar las legislaciones de todos los Estados parte.

Así pues, el Convenio brinda herramientas de ayuda como las siguientes:

- Cooperación entre los operadores de justicia, logrando mejorar significativamente las normas procesales en cada Estado.
- Común tipificación de los delitos informáticos entre los Estados parte.

En este sentido, el Convenio de Budapest es capaz de garantizar una efectiva lucha contra la ciberdelincuencia, en base a la "(...) cooperación internacional reforzada, rápida y eficaz en materia penal."[17]

En conclusión, la adhesión de los Estados al Convenio de Budapest les permite ampliar su regulación interna y hacerla más específica. Ello con el fin de tener una regulación normativa conforme a las nuevas tecnologías y, a su vez, incrementar la confianza y seguridad ciudadana frente al vertiginoso avance de las TIC.

1.3. Los delitos informáticos en la legislación peruana

Han existido diversos puntos de vista sobre cómo deben conceptualizarse los delitos informáticos, tal como se mencionó en los antecedentes del presente trabajo de investigación, al mencionar que el Código Penal peruano, en su artículo 183, inciso 3, regulaba estos delitos como simples agravantes del delito de hurto. Sin embargo, esta conceptualización ha ido progresando y enfocándose en diferentes aspectos de la cibercriminalidad.

Cabe mencionar que, según el análisis de la Ley N° 30096, se puede interpretar que el delito informático es toda aquella conducta ilícita que se materializa mediante la utilización de tecnologías de la información. En específico, se vulneran los siguientes aspectos:

- Los datos y sistemas informáticos.
- La indemnidad y libertad sexual de los menores.
- La intimidad y secreto de las comunicaciones.

[17] Consulado de Europa, *Convenio Sobre la Ciberdelincuencia* (Budapest: Serie de Tratados Europeos Nº 185, 2001) 1.

- El patrimonio, referido al aprovechamiento ilícito en perjuicio de un tercero.

-La fe pública, referida a la suplantación de identidad.

Asimismo, los autores Blossiers Mazzini y Calderón definen al delito informático como aquella acción dolosa (consciente y voluntaria), que tiene como finalidad causar perjuicio a un sujeto de derecho, realizándose el hecho ilícito a través de la utilización de dispositivos informáticos, siendo sistemas automáticos o diferentes equipos tecnológicos.[18]

En la misma línea de ideas, Arbulú Martínez conceptúa al delito informático como "(...) todo comportamiento típico, antijurídico, culpable realizado a través de sistemas de procesamiento de datos**,** contra la información automatizada siempre en perjuicio de una persona natural o jurídica. Uno de los signos característicos del delito informático es que es pluriofensivo toda vez que puede ir contra el patrimonio, la intimidad, la seguridad pública, y la seguridad informática, esta última que puede ser considerada como un nuevo tipo de bien jurídico que debe ser tutelado penalmente."[19]

En mi opinión, esta última definición es la más acertada, pues toma en cuenta los nuevos aspectos incluidos en la Ley N° 30096 y su modificación por la Ley N° 30171, referidos a su característica de pluriofensivo, ya que vulnera diversos derechos fundamentales en todas sus dimensiones, como son los datos personales y/o patrimoniales y sistemas informáticos, la indemnidad y libertad sexual, la intimidad y secreto de las comunicaciones, el patrimonio y la fe pública.

1.3.1. Legislación nacional aplicada a los delitos informáticos

La legislación peruana sobre delitos informáticos ha ido evolucionando a lo largo del tiempo, a medida que avanzaba la tecnología. Los hitos legislativos más relevantes son los siguientes: la Ley N° 30096, Ley de delitos informáticos, promulgada en octubre del año 2013, así como su modificatoria realizada a través de la Ley N° 30171, del año 2014. Ambos cuerpos normativos son de suma importancia ya que tienen la finalidad de crear un marco común de derecho sustantivo penal en relación al cibercrimen. Cabe señalar también que se utilizan los mismos principios rectores contemplados en el Convenio de Budapest.

---

[18] Juan Blossiers, Sylvia Calderon, *Delitos Informáticos (En la Banca), (*Lima: Rao, 2000),33.

[19] Víctor Arbulú Martínez, *Temas de derecho informático: Delitos informáticos, contratación electrónica, protección jurídica de programas informáticos*, (Perú: CEPREDIM, Centro de Producción Editorial e Imprenta.-UNMSM, 2002), 21.

En suma, las modificaciones normativas de la regulación de los delitos informáticos se dieron de la siguiente forma:

- Modificación de los artículos 2, 3, 4, 7, 8 y 10 de la Ley N° 30096, Ley de delitos informáticos, respecto del acceso ilícito, atentado a la integridad de datos informáticos, sistemas informáticos, interceptación de datos informáticos, fraude informático y el abuso de mecanismos y dispositivos informáticos, por lo que se evidencia que la modificación corresponde a la incorporación de dos términos: "deliberada" e "ilegítima"; las cuales al presentarse en la acción delictiva darán lugar a la configuración del tipo penal, pues guardan relación con el dolo (conocimiento y voluntad); asmismo, estos términos son determinados bajo las directrices del Convenio de Budapest.[20]
- Derogación del artículo 6**,** el cual hacía mención al tráfico ilegal de datos, porque se incorporó al Código Penal el artículo 154-A, relativo al tráfico ilegal de datos personales.
- Incorporación del artículo 12, el cual exime de responsabilidad a quien realice las conductas mencionadas en los artículos 2,3,4 y 10, referidos a la integridad de datos y sistemas informáticos y también respecto al abuso de mecanismos siempre y cuando se fundamenten en una conducta legal, con autorización de autoridad competente, con el fin de ingresar y actuar medios de pruebas u otro procedimiento.
- Modificación de la tercera, cuarta y undécima disposiciones complementarias finales de la Ley N° 30096, que versaban de forma correlativa sobre coordinación interinstitucional entre la Policía Nacional, el Ministerio Público y otros organismos especializados, cooperación operativa, regulación e imposición de multas por el Organismo Supervisor de Inversión Privada en Telecomunicaciones; esta última modificación hace referencia a la sanción administrativa, la cual se gradúa de acuerdo a la escala de multa, configurándose dicha sanción cuando se incumple la obligación prevista en el numeral 4 del artículo 230 del Código Procesal Penal.
- Del Código Penal se modificaron los artículos N° 158, 162 y 323 y se incorporaron los artículos 154-A y 183-B en el Código Penal, por lo que sólo los artículos N° 158 y 162, referidos respectivamente el ejercicio de la acción privada y la interferencia telefónica, son relevantes para el presente trabajo de investigación.

[20] Felipe Villavicencio Terreros, *Derecho Penal: Parte general (*Perú: Grijley, 2013) 354.

- En cuanto al artículo 158 del Código Penal, que establecía que los delitos sobre violación de la intimidad son perseguibles por acción privada, el artículo 154-A pasa a regular a ese delito como no perseguible por acción privada.
- El artículo N° 162 del Código Penal, relativo al delito de interferencia telefónica, fue modificado por la Primera Disposición Complementaria Modificatoria del Decreto Legislativo N°1182, y terminó redactado de la siguiente manera:

"El que, indebidamente, interviene o interfiere o escucha una conversación telefónica o similar, será reprimido con pena privativa de libertad no menor de cinco ni mayor de diez años. La pena privativa de libertad será no menor de diez ni mayor de quince años:

1. Cuando el agente tenga la condición de funcionario o servidor público, y se impondrá además la inhabilitación conforme al artículo 36, incisos 1, 2 y 4.
2. Cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con la Ley 27806, Ley de Transparencia y Acceso a la Información Pública.
3. Cuando el delito comprometa la defensa, seguridad o soberanía nacionales. Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores."

- Entonces, la modificación logra corregir la ambigüedad de este artículo, referente a la facultad del juez de discernir si la información era reservada, secreta o confidencial; empero, ahora se precisa los tipos de información que pueden ser vulnerados, y el mismo artículo menciona que todo lo referido a la información se interprete a través de la Ley N° 27806, Ley de transparencia y acceso a la información pública, pues regula el ejercicio del derecho al acceso a ese tipo de información.

- En lo que respecta a la incorporación del Artículo 154-A, su tenor literal es similar al de la Ley N° 30096: "El que ilegítimamente comercializa o vende información no pública relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análoga sobre una persona natural, será reprimido con pena privativa de libertad no menor de dos ni mayor de cinco años".[21]

[21] Código Penal Peruano, Titulo IV, promulgado el 03 de abril de 1991.

- Por su parte, el artículo 183-B está referido a sancionar la conducta de quien establece contacto o comunicación con un menor de catorce años, a fin de obtener material de connotación pornográfica, con el objetivo de obtener un aprovechamiento económico. Esta nueva concepción la vemos reflejada en base a la modificatoria realizada por la Ley Nº 30963, pues genera un mayor aporte y precisión de la conducta ilícita (proposiciones sexuales a niños, niñas y adolescentes). Asimismo, se clasifica como un delito de resultado cortado donde el agente busca un resultado que está más allá del tipo, el cual es obtener material pornográfico o tener un acto sexual con la menor, considerándose además un aprovechamiento económico, todo ello con el aporte del sistema tecnológico.

- Modificación del artículo 230, numeral 4 del Código Procesal Penal, referido a la obligación de aquellas empresas que brindan servicios de telecomunicación a guardar el secreto de comunicaciones, salvo en el caso que sean citadas como testigos de algún proceso, dictado a través de una resolución judicial, pudiendo revelar grabaciones o registro de las comunicaciones que hayan sido ordenadas mediante referida resolución.

1.3.2. Bien Jurídico Tutelado

Analizar el bien jurídico tutelado en los delitos informáticos requiere considerar la orientación político-criminal del legislador, plasmada en específico en la Ley N° 30096, Ley de delitos informáticos, en la que sus conductas típicas, colisionan en diversos intereses colectivos, por lo que se configuran dos dimensiones de los derechos que se desarrollan en los delitos.

La primera dimensión en el ámbito de la información es el espacio de contención de datos, los mismos que pueden obtenerse a través de procesos informáticos automatizados que permiten acopiar todo aquello que se pueda conocer y obtener de un determinado sujeto, siendo esta información reunida susceptible a ser tratada y difundida por medio de sistemas tecnológicos que la contienen. Esta situación tiene especial importancia ya que al obtener de manera ilícita la mencionada información, la cual es personalísima e intrínseca de un sujeto, se produce un perjuicio a otros derechos como la indemnidad sexual, intimidad, confidencialidad de los datos, seguridad del tráfico jurídico, etc.

Luego, la segunda dimensión emana de la obtención de aquella información personalísima de un determinado sujeto por terceras personas no legitimadas para darle trato, pero que enlaza a un valor económico, de modo que también se fundamenta que la información

sea considerada como bien jurídico tutelado. Tal y como lo menciona el autor Durand Valladares, uno de los bienes jurídicos tutelados es el derecho a la información, pero estos datos contienen un valor económico; por consiguiente, la información es un bien jurídico tutelado, ya que va más allá de ser simple información.[22]Todo ello siempre y cuando dichos datos personales y/o patrimoniales reflejan la esfera privada de cada persona.

De esta manera, el bien jurídico protegido conlleva la protección del patrimonio económico, ya que el sujeto pasivo tiene el derecho de propiedad frente a sus bases de datos informáticas. Es por ello que se señala que los delitos informáticos son pluriofensivos[23], ya que se afectan diversas áreas de la información; en otras palabras, ataca a más de un bien jurídico a la vez, sin perjuicio de que los bienes estén independientemente tutelados por otro tipo penal.

1.3.3. Finalidad y objeto de la Ley N° 30096

Los objetos de la Ley N° 30096, Ley de delitos informáticos, son los siguientes:

- Lograr la armonización de las normas penales peruanas con lo estipulado en el Convenio de Budapest, desplegando los beneficios de la cooperación internacional.
- Prevenir y sancionar todas las conductas ilícitas que afectan sistemas y datos informáticos, así como otros bienes jurídicos de relevancia penal, incluyendo el secreto de las comunicaciones, el patrimonio, la fe pública y libertad sexual cometidas mediante la utilización de las TIC.

Respecto de la finalidad de la Ley N° 30096, se busca combatir las conductas ilícitas referente a los delitos informáticos, tipificados por el Estado peruano, mediante el marco normativo que actualmente se vincula con la normativa extranjera, gracias al aporte brindado por el Convenio de Budapest y su beneficio en la cooperación entre Estados, el cual posee carácter transfronterizo, generando un contacto fluido entre los Estados parte.

Además, con la Ley N° 30096, el Perú logra incorporar una regulación similar a la de los demás Estados parte del Convenio de Budapest, con el propósito de sancionar la comisión de los delitos informáticos.

---

[22] Raúl Durand Valladares, "Los delitos informáticos en el Código Penal Peruano*" Revista Peruana de Ciencias Penales*, Nº. 11(2002):315- 320.

[23] María, Gutiérrez, *Fraude Informático y estafa*, (Madrid: Centro de Publicaciones del Ministerio de Justicia, 1991) 210.

Capítulo II: El delito de fraude informático en el Perú

2.1. Tipificación del Fraude Informático en el Perú

Como se mencionó en el capítulo anterior, el avance de la tecnología ha permitido la evolución de los delitos informáticos, pero a su vez la identificación de su desarrollo. Este es un caso particular de un fenómeno general: si conocemos el comportamiento repetido (el delito), se reforzarán naturalmente los mecanismos que la ley establece para combatir el cibercrimen[24] de modo que podemos partir de una concepción inicial de cibercriminalidad desarrollada por Miró. Para este autor, un cibercrimen es

"cualquier delito en el que las TIC juegan un papel determinante en su concreta comisión, que es lo mismo que afirmar que lo será cualquier delito llevado a cabo en el ciberespacio, con las particularidades criminológicas, victimológicas y de riesgo penal que de ello se derivan".[25]

Ahora bien, originalmente, el Código Penal peruano, en su Título V, Capítulo X, artículos 207-A al 207- D, dentro de la regulación contra los delitos informáticos, incluyó por primera vez el fraude informático en la legislación nacional. El texto original era el siguiente:

> *"El que, a través de las tecnologías de la información o de la comunicación, procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días multa.*
>
> *La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social."*

Sin embargo, y como se ha desarrollado previamente, la suscripción del Convenio de Budapest por parte del Estado peruano implicó la incorporación del contenido del tratado a la

---

[24] Fernando Miró Linares, "La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen," *Revista electrónica de la ciencia penal y criminología*, (2011): 2 http://criminet.ugr.es/recpc/13/recpc13-07.pdf

[25] Fernando Miró Linares, *Fenomenología y Criminología de la delincuencia en el ciberespacio, (*Madrid: Ediciones Jurídicas y Sociales S.A.C, 2012) 10.

normativa nacional. El Convenio contempla la conducta referida al fraude informático en su artículo N° 8, cuyo tenor literal es el siguiente:

> *"Las Partes adoptarán las medidas legislativas o de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causan perjuicio patrimonial a otra persona mediante:*
>
> *a. La introducción, alteración, borrado o supresión de datos informáticos.*
> *b. Cualquier interferencia en el funcionamiento de un sistema informático con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona"*

Es por ello que, de acuerdo a lo establecido en el Convenio, el Código Penal fue modificado por el Artículo 1 de la Ley N° 30171, publicado el 10 marzo del 2014, cuyo texto es el siguiente:

> *"El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días-multa. La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días-multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social."*

A la redacción se han incorporado los términos "deliberada e ilegítimamente", los cuales hacen referencia a la intención y dolo (conocimiento y voluntad), guardando relación con lo estipulado en el Convenio de Budapest. Asimismo, los términos "introducción, alteración, borrado, supresión", se encuentran en el tipo penal de fraude informático, con lo que se puede concluir que se ha incorporado de forma correcta las directrices del Convenio en el marco normativo peruano mediante la Ley N° 30096 y su modificatoria, la Ley N° 30171.

Bajo la razonable suposición de que la tipificación del Convenio es superior a la nacional, este sería un caso en el que se ve un desarrollo positivo del ordenamiento doméstico gracias a la coordinación internacional.

2.2. Fraude Informático y Estafa

Antes de realizar el análisis correspondiente al tipo penal ya referido, es importante detenernos un momento para considerar la relación entre el fraude informático y la estafa. Antes de la incorporación de tipos penales contra la cibercriminalidad, el tipo penal que más se acercaba a contemplar la conducta ahora conocida como fraude informático era el correspondiente a la estafa.

Para el caso del fraude informático, tenemos que este comprende una acción u omisión que consiste en eludir las disposiciones legales, penales o civiles, lo cual produce un perjuicio contra el Estado o terceros. Jiménez los clasifica de la siguiente forma:

1) Alteración del acceso a datos de manera ilegal.

2) Destrucción, suprimir o robo de datos.

3) Alteración o borrado de archivos.

4) Alteración o el uso indebido de sistemas o software, reescribiendo códigos con fines ilícitos.[26]

En contraste, Creus entiende a la estafa como un hecho por el que una persona, mediante la acción del sujeto activo, es inducida a error; y éste deriva en una disposición patrimonial perjudicial, siendo que el agente o sujeto activo lo realizó a fin de obtener un beneficio propio o de un tercero.[27]

En tal sentido, es importante señalar la diferencia entre ambos tipos penales. Principalmente, deben distinguirse según

> "el objetivo que se persigue, es decir, si el estafador trata de manipular a una persona, mediante engaño suficiente, se considera por lo general que se trata de un delito de estafa. Mientras que en el fraude informático el objetivo apunta a los sistemas informáticos o de procesamiento de datos, es decir, la manipulación de sistemas informáticos con propósitos fraudulentos que generen perjuicio en el patrimonio de terceros".[28]

---

[26] Juan Carlos Jiménez Herrera, *Manual de Derecho Penal Informático,* (Lima: Jurista Editores EIRL, 2017) *461*.

[27] Carlos,Creus, *Derecho penal Parte especial*, 6ta edición, Tomo I (Buenos Aires: Astrea, 1998) 104-115.

[28] Conapoc, *Diagnóstico Situacional Multisectorial sobre la Ciberdelincuencia en el Perú*, (Lima: Minjus, 2020) 31.

En ese orden de ideas, el elemento esencial diferenciador entre la estafa y el fraude informático es el engaño, pues en la estafa se induce a error a un sujeto, mientras que el fraude informático no requiere de un engaño propiamente.

En efecto, es preciso señalar la diferencia entre el sujeto pasivo del delito y el sujeto pasivo de la acción delictiva. Como señala Villavicencio, "(…) el primero es el titular del bien jurídico tutelado penalmente que ha sido lesionado o puesto en peligro por la conducta delictiva. El segundo es la persona en quien recae de manera directa la acción delictiva".[29]

Esta diferencia no se da en todos los delitos. Por ejemplo, en el delito de homicidio, el titular del bien jurídico protegido y a quien se le produce el daño son la misma persona, pues el bien jurídico protegido es la vida humana y el titular de este es la persona (sujeto pasivo del delito) y sobre quien recae el delito es la persona (sujeto pasivo de la acción). Sin embargo, en el delito de estafa sí puede distinguirse entre el sujeto pasivo de la acción y el sujeto pasivo del delito.

El sujeto pasivo del delito de estafa es el titular del bien jurídico protegido; por ejemplo, cuando se induce al engaño a un trabajador, quien realiza transferencias de dinero provocando daño o detrimento a la economía de su empleador. En consecuencia, en este caso, el sujeto pasivo del delito es el empleador, ya que es el titular del patrimonio (en este caso, dinero). Por otro lado, el sujeto pasivo de la acción es el trabajador engañado; sobre quien recae de manera directa la acción delictiva.

Habiendo realizado esta distinción, cuya materialización depende del caso concreto, podemos pasar a realizar el análisis típico penal del fraude informático.

2.3. Análisis del Tipo Penal

Bramont Arias indica que el tipo penal "se identifica con el comportamiento descrito por la ley, es decir con el supuesto de hecho típico del delito."[30] En otras palabras, el tipo penal es la descripción taxativa del comportamiento delictivo, individualizando las conductas penales relevantes prohibidas por la norma.

Debe tenerse en cuenta también que la descripción de la conducta no puede ser demasiado precisa o cerrada, ya que se correría el riesgo de que algún supuesto de hecho no se

[29] Felipe Villavicencio Terreros, *Derecho penal básico*, (Lima: Pontificia Universidad Católica del Perú, 2019) 28.

[30] Luis Bramont – Arias, "Teoría General del Delito: El tipo penal*", Derecho y sociedad:* (1996): 190.

encuentre dentro de la descripción legal y, en consecuencia, queden impunes ciertos comportamientos. Por ello, la tipificación, al menos hasta cierto punto, debe ser abstracta, a fin de englobar en ella la mayor cantidad de conductas posibles con características comunes que configuraron el hecho delictivo, tales como la forma, modo, etc., y permitir que el juzgador realice la valoración correspondiente sobre la conducta concreta a efectos de dilucidar si configura una conducta delictiva. Lo anterior tiene concordancia con García, quien establece tres funciones de la tipicidad: político-criminal, encargada de definir la conducta penalmente sancionada vinculando la conducta delictiva y la pena a imponerse; sistemática, establece elementos que permiten determinar de qué delito específicamente se trata; y dogmática, determina el objeto del dolo consumado por el autor.[31]

Cabe analizar que el tipo penal del delito de fraude informático está regulado en el artículo 8 de la Ley Nº 30096, modificado por la Ley Nº 30171, de la siguiente manera:

> *"El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, (...)."*

A continuación, se pasará a analizar el delito de fraude informático bajo el enfoque de tipicidad objetiva y subjetiva.

2.3.1. Elementos objetivos de la tipicidad penal

La tipicidad penal objetiva es la acción que procede del mundo externo, siendo perceptible por los sentidos[32]; por lo tanto, tiene la característica de ser tangible, externa y material, cual representación de cosas, hechos o situaciones de la realidad.[33] La acción humana delictiva debe cumplir entonces con la estructura de tipo, identificando el verbo rector y circunstancias tales como el tiempo, medio, modalidad, entre otras. A continuación, se pasará a detallar cada uno de esos elementos.

---

[31] Percy García Cavero, *Derecho Penal Parte General*, 3ra Edición, (Perú: Ideas Solución Editorial SAC, 2019) 393-394.

[32] José María Rodríguez Devesa, *Derecho Penal español: Parte General*, (Madrid: Artes Gráficas Carasa, 1981) 145-146.

[33] José Arigaby Molina, *Derecho penal: Parte General*, (Buenos Aires: Ediar,1972) 250.

2.3.1.1. Verbo rector. La acción u omisión es expresada gramaticalmente por un verbo, que vincula la conducta realizada por el sujeto activo en perjuicio del sujeto pasivo.

Sujeto activo: Individuo, agente o autor que realiza la acción u omisión descrita por el tipo penal, por lo que se debe tomar en cuenta que se identificarán de forma diferente cuando se analice los delitos propios e impropios. Los propios son aquellos en los que el sujeto activo tiene una condición especial (por ejemplo, la de funcionario o servidor público); mientras que los delitos especiales impropios están referidos a la relación entre el agente activo y pasivo del delito (por ejemplo, el delito de parricidio).

En el delito de fraude informático, el sujeto activo es toda aquella persona que deliberada e ilegítimamente introduce, altera, borra, suprime, clona, interfiere o manipula datos del sistema informático, mediante el uso de un aparato tecnológico, obteniendo así provecho económico. Como señala Miró, "al hablar de un cibercriminal nos referimos a cualquier sujeto que delinque utilizando el ciberespacio, por lo que no es posible una caracterización general del cibercriminal, excepto en lo relativo a que debe usar la tecnología informática con acceso a las redes telemáticas."[34]

Sin embargo, un sector de la doctrina opina que el autor de los delitos informáticos debe tener conocimientos especializados en nuevas tecnologías. En el caso del *ciberburrier*, cuya participación reside tan solo en enviar por canales seguros el dinero que recibió, fruto del delito de fraude informático. Como se evidencia, es una conducta que no requiere especialización en informática. Esta y otras complicaciones serán objeto de análisis en el tercer capítulo.

Sujeto pasivo: Aquella persona sobre quien recaen las consecuencias de las acciones delictivas, configurándose como víctima. Miró asevera que "cualquier usuario de Internet, cualquier persona que tenga un sistema informático conectado a una red o que a través de los sistemas existentes en colegios, bibliotecas, universidades, instituciones públicas, cibercafés, hoteles y demás, puede ser víctima de cibercrímenes de muy distinto tipo, dependiendo de la motivación del sujeto que realiza el ataque pero, también, del tipo de actividad que el propio usuario realice"[35]

Adicionalmente, algunos autores subclasifican al sujeto pasivo según la taxonomía ya introducida de sujeto pasivo de la acción y sujeto pasivo del delito. El sujeto pasivo de la acción

[34] Miró Linares, Fernando, *Crimen, Oportunidad y Vida Diaria*, (Madrid: Dykinson, 2015), 434.

[35] Miró, *Fenomenología y Criminología de la delincuencia en el ciberespacio,* 261

en el delito de fraude informático podría variar, dependiendo de quién sea el poseedor mediato del bien jurídico protegido. Por ejemplo, el bien jurídico protegido en el delito de fraude informático es el patrimonio, considerando como poseedor mediato al banco (en el caso de dinero), que es la entidad que lo custodia, por lo que el sujeto pasivo de la acción es la entidad bancaria. El sujeto pasivo del delito es aquella persona que es el titular del bien jurídico; es decir, es la persona a quien que se le ha alterado, borrado, suprimido o clonado los datos u otra forma de interferencia o manipulación en el sistema informático, con el uso de dispositivos tecnológicos. En el delito del fraude informático, el sujeto pasivo del delito es el titular de la cuenta bancaria, quien sufrió el detrimento económico.

2.2.1.2. Circunstancias. Las circunstancias aluden al contexto en el que se realizó el hecho delictivo. Su correcta identificación ayudará a que los hechos deben ser reconstruidos en el juicio, a través de las pruebas y que las mismas contienen: acciones, circunstancias de modo, tiempo y lugar [36]

El lugar donde se realiza el delito bajo análisis es el ciberespacio (también conocido como espacio virtual),cuya existencia y término se da en el momento en que se agota la relación de comunicación de los sujetos, entendiéndose que sin interacción no hay red, por lo cual en el caso del fraude informático, al producirse a través de transferencias bancarias, las cuales se dan a través del ciberespacio, se concluye que se producen a través de redes que unen el espacio virtual y lo físico porque se producen en sistemas informáticos ubicados en espacios terrestres.[37]

El tiempo, tiene gran importancia dentro del ciberespacio, pues es necesario determinarlo para personas que no se encuentran físicamente cerca. Usualmente los delitos informáticos se dan con la instantaneidad que facilitan las TIC, y el fraude informático no es una excepción.

Los medios de realización del delito están referidos a la utilización de medios informáticos, siendo estos aparatos tecnológicos de distintos tipos, como las computadoras, teléfonos celulares, etc. Mientras que el modo está referido a la forma en que se produce el resultado. En el caso del fraude informático, se produce mediante el diseño, introducción, alteración, borrado, supresión, clonación, interferencia o manipulación de datos informáticos.

---

[36] Oscar Peña Gonzáles, *Teoría del delito: manual práctico para su aplicación en la teoría del caso,* (Perú: Asociación Peruana de Ciencias y Conciliación - APECC., 2010), 247

[37] Miró, *Fenomenología y Criminología de la delincuencia en el ciberespacio,* 27-28

La modalidad más usual es la del phishing, que consiste en "el envío masivo de mensajes que, aparentemente provienen de fuentes fiables, con la finalidad de conseguir que el usuario proporcione datos confidenciales (ejemplo: contraseña de su cuenta de ahorro). El caso más típico de phishing es el envío de correos electrónicos que se hacen pasar por procedentes de una entidad bancaria online, para conseguir que el usuario introduzca sus contraseñas en una página web falsa"[38].

2.3.1.3. Resultados. Los resultados se refieren a una merma en el bien jurídico tutelado, motivo por el cual esos actos delictivos son llamados delitos materiales o delitos de resultado. De la misma forma lo concibe Muñoz Conde: "cuando aquí se habla de resultado se alude al resultado como modificación producida en el mundo exterior, distinta idealmente de la acción misma. En algunos delitos se exige para la consumación del tipo esta modificación separada de la acción y en este sentido se habla de delitos de resultado (…)."[39] En el caso del delito de fraude informático, el resultado es la pérdida total o parcial de bienes patrimoniales o extrapatrimoniales.

En conclusión, el resultado se puede definir como el efecto -relevante según ley penal- producido en la realidad por una acción u omisión dependiente de la voluntad del sujeto activo, lo que genera una disminución en el bien jurídico tutelado del sujeto pasivo. Por ello, el delito de fraude informático debe ser considerado un delito de resultado, pues se requiere, como presupuesto esencial, que la acción ilícita genere un perjuicio a terceros. De no materializarse este presupuesto, se identificaría como tentativa, "por lo que se le atribuye al sujeto activo la creación de un riesgo prohibido, con ausencia de la realización del mismo en el resultado previsto por el tipo penal."[40]En el tercer capítulo ampliaremos su desarrollo en función de las eventuales actuaciones del *ciberburrier*.

2.3.2. Elementos subjetivos de la tipicidad penal

El elemento subjetivo hace referencia al dolo y a la culpa del sujeto activo. El Código Penal peruano no define al dolo ni tampoco a sus elementos; sin embargo, en la doctrina y jurisprudencia encontramos un debate entre la teoría volitiva y la teoría cognitiva del dolo. Para la presente investigación, tomaré la postura de la teoría cognitiva del dolo que recientemente la Corte Suprema de la República del Perú ha asumido; es decir, que el dolo es solo conocimiento

[38]Juan Carlos Jiménez Herrera, *Manual de Derecho Penal Informático*,62.
[39] Francisco Muñoz Conde, *Teoría General Del Delito*, (Santa Fe de Bogotá-Colombia: Editorial Temis S. A, 1999) 38- 39.
[40] García Cavero, *Derecho Penal Parte General*, 459.

y que actúa con dolo la persona a la cual se le puede atribuir el conocimiento de realizar un comportamiento que crea un riesgo prohibido, el cual quiere ser evitado por el tipo penal.

Ahora bien, al atribuir un comportamiento a título doloso, se debe analizar que el sujeto activo pueda reconocer el carácter ilegal de su actuación, de tal manera que pueda tomar la decisión de desistir de cometerlo. Así, en el delito de fraude informático, el sujeto activo debe tener el conocimiento que, al *diseñar, introducir, alterar, borrar, suprimir, clonar datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático*, provocará un ilícito penal y que su comportamiento integra una conducta delictiva. Puesto que, al tener el conocimiento alcanzado a través de una percepción sensorial o la utilización de ciertas referencias, hacen comprender al autor que lleva a cabo la configuración del hecho ilícito. Cabe mencionar que, en el delito de fraude informático, debe estar presente al mismo tiempo la realización de la conducta típica, y no cabría la posibilidad de dolo antecedente ni dolo subsecuente.[41]

La doctrina también clasifica al dolo en dolo directo de primer grado (el autor conoce que su conducta puede configurar el resultado típico y quiere realizar el resultado típico), dolo directo de segundo grado (el autor tiene la intención o propósito, pero no necesariamente se realiza el tipo, sino la consecuencia de otro objetivo que conoce y va unido a este, además acepta la producción del resultado típico), y dolo eventual (el autor conoce que su conducta puede configurar el resultado típico, pero no quiere realizar el resultado típico; sin embargo, asume la producción del mismo)[42].

En el caso del delito de fraude informático, se configura el dolo directo en primer grado, excluyendo la configuración del dolo eventual, ya que la ley determina como condición de punibilidad el comportamiento de obtener para sí o para otro un provecho ilícito, determinándose el *animus lucrandi*.

Culpa. Tradicionalmente la culpa es considerada como la falta de previsión de un resultado, el cual puede ser cometido por imprudencia o negligencia en la conducta de la persona.[43] Para que se produzca, debe ser analizado el deber objetivo de cuidado y la previsión del delito; es decir, la autoridad judicial debe recurrir a las máximas de la experiencia[44].

---

[41] Ivan Meini Mendez, *Lecciones de Derecho Penal, Parte General*, (Lima: 2014) 41-45.
[42] Romy Chang Kcomt, "Dolo eventual e imprudencia consciente: reflexiones entorno a su delimitación", *Derecho y Sociedad* N° 36 (2011): 257-258.
[43] Marco Antonio Terragni, *El Delito Culposo*, (Chile: Editorial Rubinzal –Culzoni, 1984) 280-285.
[44] José Hurtado Pozo, *Manual del Derecho Pena*l, 3ra Edición, (Perú: Editora Jurídica Grijley E.I.R.L., 2005) 603-607.

La diferencia entre dolo y culpa, según Sánchez, está en que "lo específico del dolo es que el sujeto que actúa dolosamente conoce el significado típico de la conducta que realiza voluntariamente y el sujeto imprudente desconoce en toda su dimensión ese significado"[45].

Finalmente, conforme al análisis realizado en el apartado sobre la tipicidad subjetiva, el fraude informático solo puede cometerse en la modalidad de dolo. Ello excluye la modalidad culposa, porque no es posible acceder, suprimir, borrar o clonar datos informáticos, u otras actividades similares, sin tener el conocimiento y la intención para ello.

2.4. Aspectos procesales y medios probatorios digitales

2.4.1. Proceso penal

El proceso penal inicia con la vulneración de la norma y concluye con la aplicación de la sanción respectiva, y para ello debe existir un conjunto de actos previos que se analizarán en el curso del proceso, por lo que, para Vásquez, el derecho procesal penal es el

> "conjunto de disposiciones jurídicas que organizan el poder penal estatal para realizar (aplicar) las disposiciones del ordenamiento punitivo. Para ello estructura, normativamente, el aparato de investigación, juzgamiento y los procedimientos seguidos desde que se tiene información sobre un hecho presuntamente delictivo, hasta la resolución conclusiva y posterior ejecución de lo dispuesto"[46].

En otras palabras, es un conjunto de actos realizados por jueces, fiscales, defensores e imputados, etc., con la finalidad de constatar si los presupuestos que habilitan imponer la pena existen y, en consecuencia, se verifique la sanción de forma cualitativa y cuantitativa, pues el derecho procesal cumple tres funciones.

La primera es la aplicación del derecho penal material, que fija los elementos del hecho punible, los presupuestos de las consecuencias jurídicas y la determinación de la finalidad del proceso penal, por lo que constituye una conexión entre el derecho penal material y la realidad, pues transcurre desde la sospecha hasta la condena, una vez constatada la existencia del delito[47].

---

[45] Jesús María Silva Sanchez, *Aproximación al Derecho Penal Contemporáneo*, (Barcelona: Bosch, 1992) 401-402.
[46] Jorge Vásquez Rossi, *Derecho Procesal Penal*, Tomo I, (Argentina: Editorial Rubinzal –Culzoni, 1995) 34- 35.
[47] Francisco Muñoz Conde, Winfried Hassemer, *Introducción a la criminología y al Derecho Penal*, (Valencia: Tirant Lo Blanch, 1989) 120-123.

La segunda función es la protección personal, que se refiere al resguardo de los derechos de las víctimas (sujetos pasivos) del delito.[48] Como última función tenemos a la recomposición de la paz social, instaurando y reconstruyendo la seguridad ciudadana, lo que genera lograr el orden social de la comunidad.[49]

Por consiguiente, las normas de derecho procesal penal regulan adecuadamente el procedimiento que dilucida la pretensión penal, mediante un procedimiento ordenado y por el que se determina la consecuencia jurídica de un hecho punible, donde sólo el juez puede dirigir el proceso penal e imponer alguna pena con base en la certeza y convicción que se haya causado en el proceso por parte del Ministerio Público y la defensa.

2.4.2. Etapas del proceso

Las etapas del proceso penal son las siguientes: investigación preparatoria, etapa intermedia, etapa de juzgamiento, y etapa de ejecución.

La investigación preparatoria es aquella etapa en la que se tiene por finalidad reunir los elementos de convicción, de cargo y de descargo; los cuales permiten que la Fiscalía decida si formula o no la acusación.

Con relación a mi objeto de estudio, es importante mencionar que, mediante Resolución de la Fiscalía de la Nación N° 1503-2020-MP-FN, del 30 de diciembre del 2020, se resolvió crear la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público con competencia nacional, administrativa y funcionalmente dependiente de la Fiscalía de la Nación. Dentro de sus principales funciones están brindar acompañamiento técnico a los fiscales en la investigación de los delitos informáticos y aquellos casos en los cuales la obtención de prueba digital sea determinante para la investigación, y coordinar con la Oficina de Cooperación Judicial Internacional y Extradiciones de la Fiscalía de la Nación para la atención de los requerimientos en el marco de la Red 24/7 del Convenio de Budapest.

En la etapa de investigación preparatoria encontramos las diligencias preliminares, que son las primeras actuaciones llevadas a cabo por el fiscal, representante del Ministerio Público, luego de la toma conocimiento de la comisión de un suceso delictivo. En ocasiones necesitará el apoyo e intervención de la Policía o de informes de las entidades que considere pertinentes a efectos del presunto delito bajo indagación. En la misma línea de ideas, Oré indica que la finalidad de las diligencias “es determinar si el fiscal debe o no formalizar la investigación

---

[48] Jaime Rios Arenaldi, “El consentimiento en materia penal”, *Revista Politica Criminal*, 1, num. 1, (2006): 2.

[49] Julio Maier, *Derecho Procesal Penal*. Tomo I, 2° edición, (Buenos Aires:Editores del Puerto, 2004) 91-93.

preparatoria."[50] Las diligencias preliminares son de obligatoria realización, a fin de iniciar el proceso inmediato o comenzar con una acusación directa y sólo entonces se procede a formalizar la investigación preparatoria.

Específicamente para el caso del fraude informático, en estas diligencias preliminares se solicita apoyo de la División de Investigación de Delitos de Alta Tecnología (DIVINDAT), órgano de ejecución de la Dirección de Investigación Criminal de la Policía Nacional del Perú, creada mediante Resolución Directoral Nº 1695-2005-DIRGEN/EMG-06AGO2005. La DIVINDAT tiene como misión realizar las respectivas diligencias relacionadas con la investigación y denuncias de los delitos informáticos, con el fin de identificar, ubicar y detener a los presuntos autores de los delitos informáticos, para ponerlos a disposición de la autoridad competente.

Desde octubre del 2013 a diciembre del 2020, la DIVINDAT registró 12,169 delitos relacionados con la Ley N° 30096, Ley de delitos informáticos. En su informe de flujo de casos, señaló el 78% (9,515 casos) de los delitos registrados por la Divindat son de fraude informático; el 13%, sobre suplantación de identidad; el 6% sobre delitos contra datos y sistemas informáticos; y el 3% corresponde a otros delitos. Asimismo, se observa que el registro de los delitos ha tenido un ritmo creciente año a año, donde los registros del 2020 representaron el 134% de crecimiento en comparación a los registros del 2017.[51]

Por otra parte, también surgen problemas en la investigación de los delitos informáticos. Por ejemplo, la recopilación de la información registrada en sistemas de índole informático colgados en la nube electrónica. Esta información puede ser de fácil acceso por cualquier persona, así como por cualquier dispositivo, vulnerándose de esta manera la custodia adecuada de los datos. Este inconveniente dificulta la investigación, ya que, al encontrarse la información en la nube, el allanamiento de los equipos informáticos se complica.

Otro inconveniente presentado se produce con la información que contienen los equipos informáticos, puesto que se encuentra cifrada o en códigos con difícil acceso, lo que genera que la investigación se alargue.

---

[50] Arsenio Oré Guardia, Giulliana Loza Davalos, "La estructura del Proceso Común en el Nuevo Código Procesal Peruano", *Derecho y Sociedad (*2005): 167.

[51] Zoraida Avalos Rivera, *"*Ciberdelincuencia: Pautas para una investigación fiscal especializada", Oficina de análisis estratégico contra la criminalidad (2021): 20 https://cdn.www.gob.pe/uploads/document/file/1669400/CIBERDELINCUENCIA%20EN%20EL%20PERÚ%20-%20PAUTAS%20PARA%20SU%20INVESTIGACIÓN%20FISCAL%20ESPECIALIZADA%20-%2015%20FEBRERO%202021.pdf

De igual modo, en la etapa de la investigación preparatoria, a raíz de la investigación surge otro obstáculo respecto a la jurisdicción, y es que en el transcurso de las diligencias preliminares se va descubriendo el lugar donde se ha cometido el delito. En ese sentido el Convenio de Budapest, en la sección tercera de su artículo 22, establece pautas para determinar la competencia jurisdiccional: el lugar donde se suscitaron los hechos punibles o la nacionalidad del presunto autor. Ante el problema de que existan varias partes que quieran reivindicar su jurisdicción, el Convenio señala en su artículo 22 inciso 5 lo siguiente: "En el caso de que varias partes reivindiquen su jurisdicción respecto de un presunto delito contemplado en el presente Convenio, las Partes interesadas celebrarán consultas, cuando ello sea oportuno, con el fin de decidir qué jurisdicción es más adecuada para entablar la acción penal".[52]

Luego de superados los obstáculos anteriormente mencionados, se da por formalizada la investigación preparatoria y el fiscal puede ahondar en el caso, realizando las diligencias de investigación que considere pertinentes y útiles dentro de los límites de ley.[53]

La etapa de investigación preparatoria finaliza cuando el fiscal considera que se logró el objetivo de la investigación, formulando la acusación o el sobreseimiento según corresponda.

2.4.3. Agravante de delitos informáticos y consumación del delito de fraude informático

Respecto a los agravantes de los delitos informáticos, la Ley N°30096, Ley de delitos Informáticos, en el capítulo VII art. 11, contempla los agravantes, regulando lo siguiente:

> "El juez aumenta la pena privativa de libertad hasta en un tercio por encima del máximo legal fijado para cualquiera de los delitos previstos en la presente Ley cuando:
>
> 1. El agente comete el delito en calidad de integrante de una organización criminal.
> 2. El agente comete el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función.
> 3. El agente comete el delito con el fin de obtener un beneficio económico, salvo en los delitos que prevén dicha circunstancia.
> 4. El delito compromete fines asistenciales, la defensa, la seguridad y la soberanía nacionales".

---

[52] Consulado de Europa, *Convenio Sobre la Ciberdelincuencia* (Budapest: Serie de Tratados Europeos Nº185, 2001) 13.

[53] Oré y Loza, "La estructura del Proceso Común en el Nuevo Código Procesal Peruano",25.

En el caso específico del delito de fraude informático refiere en el art. 8° de la Ley 30096, lo siguiente:

> "(...)La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días-multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social".

Respecto a los delitos de resultado, como el de fraude informático, se debe señalar que se requiere para la consumación del delito de un provecho ilícito que genere un perjuicio patrimonial de terceros a través de actos de manipulación o interferencia realizados en el procesamiento de datos informáticos.

2.5. Medios probatorios digitales.

2.5.1 Conceptualización del medio probatorio

Es importante tener en cuenta la diferencia entre los medios de prueba y la prueba propiamente dicha. Los primeros hacen referencia a las pruebas, pero inmersas dentro de un proceso judicial, ofrecidas y admitidas como tal. Por su parte, la prueba propiamente dicha es un instrumento sustancial, ya que tiene como fin aportar veracidad a un hecho. En otros términos, la prueba pasa a convertirse en medio de prueba cuando es ofrecida dentro de un proceso penal.

Betham define la prueba como un supuesto que se considera verdadero y de contenido verídico, siendo utilizado como fundamentación que genera credibilidad en el juez acerca de la existencia e inexistencia de un hecho.[54] Por tal motivo, la prueba no es de carácter absoluto sino relativo, ya que se requiere la intervención del juez, quien debe realizar la correspondiente subsunción legal de la materia fáctica examinada.[55] De ahí que en la etapa de investigación preliminar corresponde el término "prueba", pues dicha etapa versa sobre su recolección, mientras que el término "medio probatorio" será usado en la etapa intermedia, ya que es ahí donde son ofrecidas y admitidas, concluyendo con la valoración y actuación en la etapa de juzgamiento.

---

[54] E. Betham Jeremias, José Gomez de Castro, *Tratado de las pruebas judiciales sacado de los manuscritos,* (Madrid: T. Jordan, 1835) 19-25.

[55] A Varela Casimiro, *Valoracion de la prueba, (*Buenos Aires: Astrea,1999) 82-83.

Asimismo, las pruebas, una vez ingresadas al proceso judicial, deben cumplir con ciertos requisitos, pues dentro del proceso se exige que los medios probatorios sean pertinentes (el hecho debe aludir exclusivamente a lo que quiera probarse), conducentes o idóneos con relación a un resultado (determinar si el medio utilizado presentado o solicitado es legalmente apto para probar el hecho) y útiles o de relevancia (detallar el aporte y descubrir la veracidad del hecho que se pretende probar a fin de alcanzar certeza al juzgador). [56]

En el caso de los delitos informáticos, es oportuno indicar que, para una adecuada investigación, es imprescindible tomar en cuenta la evidencia digital. El inconveniente es que el manejo de este tipo de evidencia es totalmente distinto al de los medios probatorios físicos.

2.5.2. Medio probatorio digital respecto del Fraude Informático en el Estado Peruano

Debido a la naturaleza del delito de fraude informático en análisis, es pertinente analizar la prueba digital o prueba informática, ya que desde la década de los 90 fue considerada como aquella que resulta del tratamiento automático de la información por medio de elaboradores electrónicos basados en la regla de la cibernética.[57]

En la actualidad, nos encontramos en la era digital, en la que circulan evidencias electrónicas que pueden ser utilizadas en los procesos judiciales. Sin embargo, al tener la calidad de digitales, son vulnerables, ya que la información o datos están almacenados en el software o en algún hardware. De tal manera que será considerado como "digital" cuando tenga que probarse un suceso ilícito que se cometió a través de portales como Google, Firefox, WhatsApp, Facebook, Skype, MSN, email, o a través de dispositivos electrónicos, de uso personal, etc., pudiendo estar en diferente formato como mp3, mp4, png, archivos encriptados, etc.[58] Asimismo, pueden ser almacenados en una base de datos virtual, también llamada "nube", lo cual conlleva que, en algunos casos, su acceso sea complicado o incluso imposible.

La prueba digital es considerada un dispositivo electrónico que tiene como finalidad almacenar datos y permitir su transferencia, ya que su contenido brinda convicción respecto de una conducta, hecho y expresión de voluntad de una acción o inacción, lo que logrará acreditar

---

[56] Pablo Talavera Elguera, *La Prueba en el Nuevo Proceso Pena: Manual del derecho probatorio y de la Valorización de las Pruebas en el Proceso Penal Común*, (Lima:Academia de la Magistratura, 2009) 25.

[57] Varela, *Valoracion de la prueba,* 120-126.

[58] Joaquin Delgado Martín, "La prueba electrónica en el proceso penal", *Diario La Ley*, Nº 8167 (2013):1-3.

la comisión de un hecho ilícito. Es así que los medios de prueba digital permiten corroborar la acción delictuosa en vía judicial, de modo que se genere la debida certeza al juez.[59]

Una vez asegurada la escena del crimen y después de haber hallado, incautado o recibido los dispositivos de almacenamiento, se formularán las actas correspondientes, teniendo en cuenta si los dispositivos son transportables o no (por su volumen, limitaciones legales, funcionales, entre otros). Los dispositivos transportables serán objeto de recojo; para los dispositivos no transportables se deberá comunicar al personal policial especializado para la adquisición de la evidencia digital, así como también se analizará la posibilidad de la utilización del muestreo rápido, que consiste en la búsqueda sencilla de la estructura del aparato tecnológico.

Adicionalmente, de requerir una investigación especializada, se debe contar con autorización judicial, así como con el software necesario para realizar las copias o desencriptar los archivos materia de investigación, tomando en cuenta que se requiere de un experto informático que asegurará la integridad de la evidencia recolectada, todo ello en orden de perennizar así la escena del crimen mediante la grabación de video y la toma de vistas fotográficas (panorámicas y de detalle) antes, durante y después de las actividades realizadas; embalar y lacrar los dispositivos individualmente".[60]

Otro método de investigación es el que se realiza en vivo, siendo esta una excepción a las formas de investigación, ya que el objetivo de toda investigación es que se evite acceder al contenido de los elementos electrónicos para prevenir que sean contaminados. Sin embargo, este método es aplicado en casos de urgencia, requiriendo de una previa autorización judicial, detallando en un acta las acciones efectuadas en su totalidad y así conocer los efectos que conlleva el acceso a la prueba digital, por lo que "en el proceso de recolección de evidencia digital se debe tener en cuenta el orden de volatilidad, debiendo respetar el siguiente, ordenado de mayor a menor: a) contenido de registros, b) tablas de ruteo y memoria caché, c) procesos de ejecución, d) memoria RAM, e) dispositivos de almacenamiento masivo, f) contenedores de almacenamiento remoto, g) almacenamiento de resguardo y respaldo".[61]

---

[59] José Luis Sánchez Hernández, "WhatsApp, prueba válida en juicio" *Revista del Ilustre Colegio de Abogados de Salamanca*, nº. 12, (2016) 53.

[60] Ministerio del Interior, "Manual de Evidencia Digital", (2020): 12-13 https://cdn.www.gob.pe/uploads/document/file/1303962/DWP-ManualParaRecojo-EVIDENCIA.DIGITAL.pdf?v=1600289472

[61] Martin Alan Nessi , "Manual de evidencia digital", (2017):27 https://www.mpfn.gob.pe/Docs/0/files/manual_evidencia_digital.pdf

Es preciso señalar que toda esta información digital es considerada como elemento de convicción, que debe contar con determinada seguridad y protección. Solo así puede ser presentada en todas las etapas del proceso penal**,** incluso como prueba anticipada o prueba preconstituida. La primera puede ser actuada antes del juicio o solicitada de oficio**,** siempre que la prueba se encuentra en riesgo de desaparecer o sea posible su destrucción. La prueba preconstituida es aquella que se da fuera del ámbito del proceso de investigación, y puede ser practicada dentro de la fase de la investigación, con autorización del juez competente, para conservar o asegurar el contenido integral de las fuentes de prueba.

Los requisitos para el análisis forense se refieren a emitir un oficio precisando el objetivo de la modalidad del suceso investigado, por orden fiscal, por la cual se autoriza la participación de apoyo policial y fiscalías competentes, acopio de documentación del hecho emitiendo un acta de recojo, incautación, entrega y recepción, lacrado, cadena de custodia y su continuidad, con el fin de autorizar el análisis de los dispositivos digitales que contienen información relevante al tema investigado.[62]

De tal manera que, en nuestra legislación, la prueba digital está implícita en el artículo N°185 del Código Procesal Penal, considerando que la prueba digital es un medio probatorio documental. Sin embargo, al no tener un tratamiento especial para las pruebas digitales, estas son actuadas de la misma manera que los documentos ordinarios, mediante la palabra, el sonido y la imagen; y que al ser incorporados al proceso como una prueba documental permiten reproducir palabras, datos, información, etc., almacenadas con el objeto de lograr comprobar un determinado hecho ilícito. Así también el documento electrónico, considerado como un medio de prueba, reúne los requisitos establecidos por la doctrina: i) es un método de perpetuar y constatar el contenido, ii) medio de garantía para conocer al autor y iii) sirve como prueba de su contenido.[63]

Por todo ello, las pruebas digitales son consideradas pruebas independientes y autónomas, ya que su tratamiento procesal no está regulado en algún artículo del código penal de manera específica[64]; razón por la cual la doctrina sostiene y defiende la existencia de ciertas semejanzas entre la prueba digital o electrónica y la prueba documental, basándose sólo en lo

---

[62] Ministerio del Interior, “Manual de Evidencia Digital”, 37.

[63] María del Carmen García Cantizano, *Falsedades Documentales* en el Código Penal de 1995, (Valencia: Tirant lo blanch, 1997) 23.

[64] Víctor Arbulú Martínez, *Temas de derecho informático: Delitos informáticos, contratación electrónica, protección jurídica de programas informáticos,* 22.

regulado en el Artículo 185º del Código Procesal Penal. Sin perjuicio de ello, las pruebas electrónicas o digitales pueden ser corroboradas con otras pruebas de carácter documental, testimonial y sobre todo con pruebas científicas, denominadas pericia de informática forense.

La Policía Nacional del Perú, a través de la DIVINDAT, se encarga de obtener los medios probatorios ideales para que sean valorados en el proceso penal de fraude informático, en base a las siguientes pericias: "autenticación de archivos digitales en audio, imagen y video, procesamiento de imágenes digitales con fines de identificación, recuperación y búsqueda de archivos electrónicos en dispositivos tecnológicos (equipos celulares, computadoras, USB, etc.), análisis de sistemas informáticos con fines de identificar manipulaciones indebidas, recuperación de imágenes de cámaras (circuito cerrado de televisión), desbloqueo de celulares Android, iOS y otros sistemas operativos y recuperación de mensajes de textos, WhatsApp y otros".[65]

> Siguiendo la misma línea,
>
> "en caso de considerarse pertinente, contar con la autorización judicial y el software necesario, podrá decidirse con el experto informático la realización de una copia o imagen forense, en la escena de delito. La recolección de evidencia digital mediante imágenes forenses requiere de la experticia y la disponibilidad de equipamientos e insumos para su realización. Una imagen forense es una copia bloque a bloque -bit a bit- del contenido digital almacenado, el que es autenticado mediante una función HASH o digesto matemático, a fin de asegurar la integridad de la evidencia colectada. Las imágenes forenses pueden realizarse mediante una computadora y un programa, o bien, utilizando un dispositivo autónomo denominado duplicador forense. El HASH se refiere a una función o método para generar claves que representen de manera casi unívoca a un documento, registro, archivo, etc. Resumir o identificar un dato a través de la probabilidad, utilizando una función hash o algoritmo hash. El hash permite darle mayor seguridad de que la evidencia digital obtenida no fue manipulada ni alterada, ya que el HASH generado es inviolable".[66]

En consecuencia, la prueba debe contar con las medidas de seguridad necesarias, ya que se corre el riesgo de tener algún deterioro, sea por el tiempo transcurrido o en el caso de aparatos electrónicos que contengan la información que servirá como medio de prueba, sufran daño al

---

[65] Zoraida Avalos Rivera, "Ciberdelincuencia: Pautas para una investigación fiscal especializada", 28.
[66] Martin Alan Nessi , "Manual de evidencia digital", 26.

traslado realizado para iniciar con la evaluación pericial, es por ello que la forma de asegurar la prueba es mediante la cadena de custodia, técnica que "se inicia con el aseguramiento, inmovilización y/o recojo de los elementos materiales encontrados en la escena del crimen"[67]con el fin de brindar seguridad y conservación de los medios de prueba inmersos en un proceso de investigación, resguardando así su valor probatorio.

El procedimiento inicia dejando constancia detallada de cuál es el medio probatorio otorgado en custodia, debe obrar en acta de lacrado y deslacrado, con el objeto de evitar alteraciones de lo resguardado, consignando anotaciones detalladas de la descripción de la evidencia. De esta manera el medio probatorio no será contaminado.[68]

[67] Ministerio del Interior, "Manual de Evidencia Digital", 39.
[68] Hipolito Aguirre Salas, "Criminalística y cadena de custodia" *Revista de Derecho Penal y el Derecho Procesal*, (2014): 23.

Capítulo III: La responsabilidad penal del *Ciberburrier*

3.1 Conceptualización de "el *ciberburrier*"

Tomando en cuenta lo estudiado en el capítulo anterior sobre el delito de fraude informático, en el presente capítulo se analizará el comportamiento de las personas que brindan sus servicios para lograr consumar el referido delito. En particular, nos concentramos en la figura del *ciberburrier*, que es la persona que recibe transferencias dinerarias y luego envía dicho dinero, mediante depósitos o transferencias, a las cuentas indicadas por el autor del delito, a cambio de un pago por la intermediación.

El término "*ciberburrier*" es producto del americanismo "burrier", que es empleado para caracterizar a aquella persona que transporta droga, y de la palabra "ciber" que es un prefijo acortado del adjetivo "cibernético", el cual es parte de los términos relacionados con el mundo de las computadoras y de la realidad virtual. Así, el término responde a la aplicación por extensión de *burrier*, dado que se trata de un intermediario que facilita al autor el objeto del delito, y a la referencia a las tecnologías de la información, mediante las cuales se produce el delito en mención.

De ahí el motivo del uso de la palabra *ciberburrier*, pues se busca caracterizar a la persona que interviene como autor y/o partícipe en los delitos que estén vinculados con cualquier interferencia o manipulación en el funcionamiento de un sistema informático. Así, si bien aquí concentraremos nuestra atención en el *ciberburrier* en el caso del fraude informático, también puede hablarse de un *ciberburrier* que participe en delitos como lavado de activos, en los que se usen medios digitales para transferir activos, o incluso en el delito de contrabando cuando el objeto del delito sea de naturaleza informática o cibernética[69].

Miró utiliza la equivalente expresión "cibermulero", entendiéndola como:

Aquella persona también conocida como «mulas» o «muleros»; agentes que operan como intermediarios, colocando a disposición sus cuentas bancarias con el fin de recibir dinero obtenido de manera fraudulenta, ya que posteriormente lo envían mediante transferencia bancaria al sujeto que contrató sus servicios.[70]

---

[69] "Ciber burrier intentó salir de Hong Kong con 256 procesadores de PC pegados a su cuerpo", RPP, 8 de Julio de 2021 https://rpp.pe/tecnologia/pc/trafico-ciber-burrier-intento-salir-de-hong-kong-con-256-procesadores-de-pc-pegados-a-su-cuerpo-noticia-1346433

[70] Fernando Miró Linares, "Cibercrímenes Económicos Y Patrimoniales". *Memento Práctico. Penal Económico y de la Empresa* (2016): 516.

En particular, según Miró, el cibermulero brinda su cuenta bancaria para recibir transferencias del dinero obtenido fraudulentamente, y posteriormente lo entrega vía electrónica, por lo que algunas acciones mediante las que participa serían la apertura de la cuenta bancaria para recibir el dinero, la recepción del dinero objeto del delito, y la recepción de un pago por este servicio.[71]

En ese sentido, para determinar el comportamiento del *ciberburrier*, deberá evaluarse si este sujeto actuó de acuerdo con el tipo penal de fraude informático previsto en el artículo 8 de la Ley N° 30096, delito que se analizó en el capítulo anterior. Esta misma conducta será analizada desde la perspectiva de otros delitos que, *ex ante*, se podría pensar que también podrían configurarse con la conducta del *ciberburrier*: fraude informático, lavado de activos y receptación.

3.2 Formas de participación del *ciberburrier*

La participación en un hecho ilícito se determina identificando tanto a los diferentes tipos de autores del delito, así como a los intervinientes, quienes coadyuvaron a la realización del hecho delictivo, surgiendo así la figura del cómplice e instigador. El término "participación" suele ser usado en un sentido más restringido como el que comprende la complicidad e instigación; es decir, la intervención delictiva se dividiría en autoría (directa, mediata y coautoría) y participación (instigación y complicidad).[72]

Asimismo, García Cavero señala que "No basta con una simple intervención fáctica en la etapa previa o incluso en la ejecución del hecho delictivo, sino que es necesario que normativamente se considere a los intervinientes competentes por el injusto común, esto es, por la lesión de la norma. Esa competencia conjunta por el delito se produce cuando tiene lugar una división vinculante del trabajo en atención al sentido social atribuido a cada uno de los aportes realizados. Una vez determinada la competencia conjunta de los intervinientes, la distinción entre autores y partícipes dependerá de un criterio cuantitativo, pero no en función de la cantidad de intervención en el hecho, sino de la infracción del deber".[73]

---

[71] Fernando Miró Linares, "La respuesta penal al ciberfraude: Especial atención a la responsabilidad de los muleros del phishing". *Revista Electrónica de Ciencia Penal y Criminología*, (2013): 31 http://criminet.ugr.es/recpc/15/recpc15-12.pdf

[72] Villavicencio, *Derecho penal básico*, 2019, 109.

[73] García, *Derecho Penal Parte General*, 765.

En primer lugar, debemos determinar de qué manera participa el *ciberburrier* en la comisión del delito.

3.2.1 El ciberburrier como autor

El artículo 23 del Código Penal peruano introduce las nociones de autoría, autoría mediata, y coautoría de forma muy breve, al señalar que "el que realiza por sí o por medio de otro el hecho punible y los que lo cometan conjuntamente serán reprimidos con la pena establecida para esta infracción".

Dada esta limitación, la doctrina ha desarrollado teorías para determinar la configuración de cada una de estas tres figuras. La llamada Teoría del dominio del hecho, que nos ofrece métodos para determinar la configuración de cada forma de participación delictiva, ha sido adoptada en el Perú por la Corte Suprema y el Tribunal Constitucional. Sin embargo, es pertinente mencionar que hay delitos en los cuales la determinación de la autoría no se puede sustentar en el dominio del hecho, sino deberá fundamentarse en la infracción de un deber especial, como son por ejemplo los delitos realizados por funcionarios públicos. Esta bipartición ha sido explicada por García Cavero:

"El punto de partida de nuestra comprensión de la autoría es la distinción entre delitos de dominio (competencia por organización) y delitos de infracción de un deber (competencia institucional). En los delitos de dominio, el autor infringe el deber negativo de todo ciudadano de no dañar a otro. Por otro lado, en los delitos de infracción de un deber, la competencia penal del autor se determina por la infracción de deberes positivos derivados de una vinculación institucional de carácter específico".[74]

Previamente, es necesario acotar cuál es el hecho cuyo dominio determina la forma de participación. En este caso, al analizar la figura del fraude informático, y como ya se estableció en capítulos previos, el hecho es el provecho ilícito (disposición patrimonial) en perjuicio del titular de la cuenta bancaria, a través de la manipulación o interferencia del funcionamiento de un sistema informático.

Así, las formas de autoría son las siguientes:

[74] García, *Derecho Penal Parte General*, 736.

a. Autoría directa: La autoría directa es la forma de autoría que tiene lugar a través de la ejecución del hecho delictivo. Para determinar si el ejecutor directo de la conducta típica es autor del delito, es necesario cuantificar su competencia en función del dominio del riesgo prohibido.[75] Aplicándolo a la presente investigación, queda descartado entonces que el *ciberburrier* ostente el dominio completo de la comisión del delito de fraude informático, ya que solo cumple funciones intermediarias, siendo contratado por un tercero a efectos de recibir el dinero derivado de una o varias acciones ilícitas cometidas por el autor. Desde mi punto de vista, el *ciberburrier* tiene un dominio cuantitativamente menor que el autor del delito de fraude informático, pues no participa en la manipulación o interferencia del funcionamiento de un sistema informático para acceder a los datos y contraseñas del titular de la cuenta bancaria, sino que facilita que la transferencia electrónica del dinero alcance al autor del delito, quien tiene pleno control sobre el hecho.
b. Autoría mediata: La autoría mediata posee una competencia normativa u organizativa en la comisión del delito. En otras palabras, un autor mediato se vincula con quienes actúan para concretar materialmente la figura delictiva por medio de una "relación de subordinación".[76] Desde mi punto de vista, el *ciberburrier* no puede ser un autor mediato en el delito de fraude informático, pero dadas las circunstancias, si podría ser considerado el instrumento del autor mediato.
c. Coautoría: La coautoría consiste en la realización de acciones equivalentes y simultáneas por parte de todos los intervinientes en el delito, quienes ejercen de manera consciente y voluntariamente actividades equivalentes de acuerdo a una división de funciones de índole necesaria,[77] lo que presupone una estructura horizontal, e interdependencia.[78]Asimismo, la doctrina y jurisprudencia han señalado que la coautoría requiere de elementos. Por ejemplo, la Corte Suprema del Perú, en el fundamento noveno de su casación N° 1039-2016 Arequipa, señala lo siguiente:

"Noveno. Ahora bien, dicha norma regula la coautoría en base a tres requisitos: a) decisión común: entre los intervinientes existe una decisión común de realizar el delito,

[75] García, *Derecho Penal Parte General*, 738.
[76] C. Rodríguez & E. Demetrio, Curso de Derecho penal Parte General, (España: Ediciones Experiencia, S.L. ,2010) 385.
[77] Francisco Muñoz Conde E, *Teoría general del Delito*, (Bogotá: Themis,2004) 76.
[78] Claus Roxin, "Problemas de Autoría y Participación en la criminalidad organizada", *Revista Penal N*° 2, (1998): 63.

en base a una actuación colectiva orientada al logro exitoso del resultado; b) aporte especial: el aporte individual que realiza cada actuante es esencial o relevante para el logro del plan de ejecución; c) tomar parte en la fase de ejecución: cada sujeto al tomar parte en la ejecución desplegó un dominio parcial del acontecer, este requisito precisamente da contenido real a la coautoría, pues la sola intervención en la fase preparatoria no es suficiente, porque ello también existe en la complicidad e instigación, quiere decir que la participación ejecutiva de contenido final al dominio funcional al hecho en la coautoría".

En lo que respecta al delito de fraude informático, para poder considerar al *ciberburrier* como coautor del delito, tendría que ser considerado como uno de los que comete directamente el delito, supuesto descartado en el inciso "a" del presente apartado.

3.2.2 El ciberburrier como partícipe

El *ciberburrier* además podría ser considerado partícipe del hecho ilícito como cómplice o instigador, por lo que se pasará a analizar las mencionadas figuras.

3.2.2.1. Complicidad. El cómplice es la persona que aporta al delito cometido por el autor. Como ha señalado García Cavero: "La complicidad está constituida por las contribuciones o auxilios, anteriores o simultáneos, que son útiles para la realización de un delito. La utilidad del aporte puede ser potencial o efectiva, bastando con que se haya incrementado el riesgo para la víctima o la oportunidad de éxito del autor."[79]

La complicidad se encuentra regulada en el artículo 25 del Código Penal peruano:

> *"El que, dolosamente, preste auxilio para la realización del hecho punible, sin el cual no se hubiere perpetrado será reprimido con la pena prevista para el autor.*
> *A los que, de cualquier otro modo, hubieran dolosamente prestado asistencia se les disminuirá prudencialmente la pena.*
> *El cómplice siempre responde en referencia al hecho punible cometido por el autor, aunque los elementos especiales que fundamentan la penalidad del tipo legal no concurran en él."*[80]

[79] García, *Derecho Penal Parte General*, 783.
[80] Código Penal Peruano, Titulo II, promulgado el 03 de abril de 1991.

En el caso bajo análisis, el *ciberburrier* aporta a los hechos que configuran el delito de fraude informático, con base en lo instruido por el autor del delito, con el fin de recibir el dinero ilícito, para luego trasladarlo a la cuenta que le indique el autor, pero dicha participación es solo parcial, pues interviene únicamente en la recepción de los activos.

Por otra parte, con relación al grado de complicidad, la doctrina diferencia entre cómplice primario y secundario por la necesidad o esencialidad del aporte; esto es, si el acto a realizarse es un acto indispensable, sin el cual no se hubiera podido cometer el delito. Aplicándolo al caso concreto, se observa que, sin la intervención o contribución del *ciberburrier*, no sería posible conseguir el objetivo del delito. Como lo señala Miró:

> "En las conductas de los cibermuleros, el sujeto se integra, se suma, a un proyecto delictivo, a un injusto que era de otro y que, con sus actos, pasa a serle también propio. El mulero que recibe importantes ingresos y los transfiere por los medios que le han ordenado, realiza un comportamiento cuyo único sentido social es, a todas luces, hacer posible a otros sujetos determinados o indeterminados, la consumación final del delito. La intervención del mulero es casi insustituible como forma de lograr el perjuicio patrimonial por medio de la estafa informática, puesto que, si bien con la transferencia patrimonial ya se entiende producido el perjuicio, no ocurre lo mismo con el éxito del ataque para el cibercriminal que lo protagoniza y que le obliga a contar con muleros sin los cuales no obtiene las ganancias y, por tanto, no llevaría a cabo el ataque".[81]

Por su parte, un cómplice secundario sería quien coadyuva al autor del delito de forma contingente; es decir, su aporte no es indispensable para la realización del ilícito, pues de todos modos el delito se hubiera consumado. Como ya se mencionó, para el delito de fraude informático el *ciberburrier* brinda un aporte, así sea parcial, imprescindible para la consumación del hecho ilícito, por lo cual no podría figurar como cómplice secundario del delito de fraude informático.

Es importante recordar que los cómplices, en general, "ocupan un nivel inferior y sólo tienen un conocimiento necesario para prestar su colaboración, la ignorancia del resto del operativo no borra ni disminuye su culpabilidad porque fueron conscientes de la antijuridicidad

[81] Miró, "Cibercrímenes Económicos Y Patrimoniales", 516.

de su conducta, prestando su conformidad con un evidente ánimo de enriquecimiento, ya supieran, no quisieran saber –ignorancia deliberada–, o les fuera indiferente el origen del dinero".[82]

Es por ello que, desde mi perspectiva, y siguiendo a Miró, considero que el *ciberburrier* participa como cómplice primario y, por ello, debe ser sancionado "(...)dentro de los marcos penales establecidos en los tipos legales de la parte especial(...)"[83]. Para el caso del delito de fraude informático, el juez deberá evaluar las circunstancias de participación del *ciberburrier* para imponer la pena privativa de libertad, que, según hemos visto, oscila entre los 3 y 8 años, o entre los 5 y 10 años, dependiendo de la modalidad.

Sin embargo, también existe la posibilidad de que una persona reciba en su cuenta bancaria dinero sin su consentimiento, solo para posteriormente ser contactado por un supuesto titular legítimo del dinero, quien le dice que por equivocación se ha transferido dinero a su cuenta y que se lo devuelva mediante transferencia bancaria al número de cuenta que se le indicará. Obviamente, en este caso se trataría en realidad del autor de un fraude. Debe distinguirse esta posibilidad del caso de quienes actuaron a sabiendas, o pudiendo prever la ilicitud de su aporte, recibieron el dinero y consiguieron así el fin deseado por el autor del delito.

Por ello es necesario analizar si el *ciberburrier* conoce o no el significado de su intervención.

Con relación al conocimiento, Oré ha señalado lo siguiente:

> "Algunas sentencias, reseñadas por Blanco Cordero, lo hacen a través de pruebas de indicios o en aplicación del concepto de ignorancia deliberada, atribuyendo complicidad en el delito de estafa informática bajo el entendido que los muleros tenían un conocimiento suficiente de su participación en un delito de tipo informático, y que el desconocimiento – o indiferencia- del resto no borraba ni disminuía su culpabilidad porque eran conscientes de que participaban en algo ilícito. Sin embargo, esta línea jurisprudencial tropieza con el doble dolo del cómplice que tradicionalmente se exige en estos casos, es decir, el conocimiento de la propia acción y el de los elementos esenciales del hecho principal: tendría que imputarse al cibermulero, al menos, saber que el dinero que recibe y transfiere ha sido obtenido indebidamente mediante técnicas o manipulaciones informáticas; en cambio, no se exigirá el conocimiento preciso del

[82] Javier Gustavo Fernandez Peruelo, *Derecho Penal e Internet*, (España: Lex Nova, 2011), 41.
[83] Villavicencio, *Derecho penal básico*, 2019, 113.

sujeto pasivo o del autor del ataque informático, ni las características completas del injusto".[84]

Es en el conocimiento de los elementos esenciales del hecho principal donde se encuentra un problema, ya que el *ciberburrier*, al ser un intermediario, no puede presumir ni saber quién es exactamente el sujeto pasivo o el autor del delito de fraude informático, pues simplemente le interesa cumplir con la función de recibir y transferir el dinero para recibir un pago a cambio. Desde mi punto de vista, la ausencia del conocimiento del *ciberburrier* de los elementos esenciales del delito de fraude informático no constituiría una atipicidad por falta de dolo, puesto que el *ciberburrier*, con su comportamiento de recibir dinero y reenviarlo a otras cuentas a cambio de una comisión, demuestra tener un conocimiento a título de dolo eventual sobre la ilicitud de la actividad, así no sepa que proviene específicamente de un delito de fraude informático. En otros términos, al *ciberburrier* se le podría imputar el conocimiento de estar recibiendo un dinero ilícito, sin importar si posee conocimiento preciso acerca del delito que originó el dinero que recibe en su cuenta bancaria.

Por otro lado, respecto a la segunda forma de participación en los delitos, tenemos a la instigación. El Código Penal peruano, en su artículo 24, estipula lo siguiente: "El que, dolosamente, determina a otro a cometer el hecho punible será reprimido con la pena que corresponde al autor".

De este artículo se infiere que el instigador es aquél que se encarga de generar una decisión en el autor para cometer determinado delito. En este caso, el *ciberburrier* no puede ser considerado como un instigador en el delito de fraude informático, obviamente tampoco como instigado, dado que solo cumple con la función encomendada por el autor del fraude informático, que es la de recibir y enviar dinero a través de transferencias bancarias, función que como, ya se ha señalado, resulta un auxilio a la realización del delito de fraude informático, lo que se ajustaría más a la complicidad.

Ahora se procederá a analizar los delitos de receptación y lavado de activos, así como un eventual concurso de delitos, según la conducta del *ciberburrier*. La pregunta por responder es si es más exacto encuadrar la conducta del *ciberburrier* en la autoría de los mencionados delitos, o considerarse, como hasta ahora he señalado, como un partícipe del delito del fraude informático.

---

[84] Isidoro Blanco Cordero, *El delito de blanqueo de capitales* (Pamplona: Thomson Reuters Aranzadi, 2012): 708-712 citado en Eduardo Oré Sosa, *Delictum, apuntes de derecho penal*, (Perú: Editores del Centro, 2022) 270.

3.3. El *ciberburrier* como autor del delito de receptación

3.3.1. Conceptualización del delito de Receptación

La receptación es considerada "un delito dependiente de un delito previo o antecedente(...)"[85]. Asimismo, de acuerdo con lo señalado por Bajo Fernández, "es un delito que consiste sustancialmente en aprovecharse de los efectos de otro delito cometido".[86]

Por ende, la receptación hace referencia a quien, con conocimiento o presunción, oculta o encubre los efectos de un delito, o el bien u objeto que provenga de un hecho delictivo, por lo cual se puede decir que el receptador ayuda a los responsables de un delito anterior, pero en el cual no ha intervenido.

En consecuencia, para que la persona se configure como receptador, debe tener conocimiento o presumir que el bien que adquiere, recibe en prenda o guarda, esconde, vende o ayuda a negociar, proviene de un delito. Es por ello que actualmente es necesario identificar las circunstancias en cada caso concreto; por ejemplo, cuando una persona adquiera o venda bienes, debe conocer la procedencia del objeto materia de transferencia, eliminando así cualquier duda sobre su origen.

3.3.2. Regulación del delito de receptación en el Código Penal peruano y análisis del tipo penal

El delito de receptación se encuentra regulado en el Titulo V: Delitos Contra el Patrimonio, Capítulo IV: Receptación, Art. 194 del Código Penal, señalando lo siguiente:

> "El que adquiere, recibe en donación o en prenda o guarda, esconde, vende o ayuda a negociar un bien de cuya procedencia delictuosa tenía conocimiento o debía presumir que provenía de un delito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa."

Cabe mencionar que, al tipificar el delito de receptación, se tutela el patrimonio de la persona cuyos bienes fueron receptados y el orden socioeconómico, ya que la conducta ilegal genera un modo de comercio ilegal, provocando tráfico ilícito, contrabando, etc.

---

[85] James Reátegui Sánchez, *Manual de derecho penal. Parte especial Delitos contra la vida, contra el patrimonio y otros*, (Lima: Pacífico Editores. SAC, 2015) 422.

[86] Miguel Bajo Fernández, *Manual de derecho penal: Parte especial*, (Madrid: Ceura, 1990), 56.

Ahora bien, resulta trascendente analizar el delito de receptación, para verificar si la conducta del *ciberburrier* encaja en el mencionado tipo penal.

Tipicidad del delito, objetiva y subjetiva

Elemento objetivo:

En el delito de receptación, el sujeto activo es la persona que adquiere, recibe en donación o en prenda, o guarda, esconde, vende o ayuda a negociar un bien de origen delictivo. Este sujeto activo tiene conocimiento o presume la comisión de un delito, no figurando como autor ni como cómplice, y el hecho de adquirir, recibir, esconder, vender el bien debe ser posterior a la realización de dicho ilícito.[87]

Es importante recalcar que el sujeto activo no debe estar involucrado en el anterior delito, por lo que un requisito esencial para que se configure es que este no haya sido autor material o partícipe del delito antecedente. En otras palabras, "(...) dada su naturaleza de encubrimiento, contiene la receptación una exigencia negativa implícita: la de que el culpable no haya participado como autor o cómplice del delito previo"[88]. Otro aspecto importante es que la receptación solo es posible cuando el delito previo ya se ha consumado.

Por lo tanto, el *ciberburrier*, para ser considerado como autor del delito de receptación, tiene que haber recibido en donación o en prenda o guardar, esconder, vender o ayudar a negociar un bien de origen delictivo y, en adición a ello, no haber participado como autor ni partícipe en el delito previo.

Es pertinente recordar, por ello, que la consumación del delito de fraude informático se produce con el provecho ilícito en perjuicio de tercero mediante la manipulación o interferencia en el funcionamiento de un sistema informático. Este provecho ilícito se concreta cuando el autor del delito de fraude informático recibe en su cuenta bancaria el dinero. En otras palabras, el *ciberburrier* participa de manera imprescindible en el delito de fraude informático al contribuir al perjuicio patrimonial; es decir, la contribución del *ciberburrier* es anterior o simultánea a la consumación del delito de fraude informático.

De manera similar lo señala el Recurso de Nulidad N° 1923-2011, Lima Norte, en su fundamento décimo:

---

[87] Alonso Peña Cabrera Freyre, *Derecho penal. Parte especial*, Tomo II, (Lima: Idemsa, 2013) 115.

[88] Tomas Salvador Vives Antón, *Derecho Penal. Parte Especial*, (Valencia: Tirant lo blanch, 1993) 802.

Décimo.- Que, por otro lado, en lo que respecta al delito de receptación, si bien es un delito autónomo, tiene como presupuesto que se haya cometido un ilícito anterior sin cuya existencia no podría configurarse, no por ser dependiente de él, sino por la misma definición de la conducta ilícita, entendida como la lesión de un bien jurídico lesionado; que, asimismo, el sujeto activo de la receptación no debe haber intervenido ni material ni intelectualmente en la perpetración del delito precedente, mientras que el sujeto pasivo es el mismo, pues es el titular del bien jurídico protegido.

Por lo tanto, la conducta del *ciberburrier* no puede configurar una receptación, en la medida en que los actos del *ciberburrier* están enmarcados en la consumación del fraude informático y no pueden ser posteriores a este.

Elementos subjetivos:

El delito de receptación es un delito doloso, ya que se requiere del conocimiento o de la presunción de conocimiento del origen ilícito de los bienes, tal como lo menciona Rojas: "En el delito de receptación el elemento subjetivo se encuentra constituido por el conocimiento cierto o la presunción de que el bien procede de un delito anterior, y la voluntad de aprovecharse de tales efectos(...)"[89]. Por consiguiente, en este delito se desprenden dos requisitos esenciales: uno de ellos es el conocimiento o la presunción de conocimiento de la comisión de un delito, y el otro es el aprovechamiento.

Respecto al conocimiento de la comisión del delito, Peña Cabrera ha señalado que:

"Es de recibo que un tipo penal así concebido, requiere de un conocimiento efectivo y actual del agente, en cuanto a la procedencia delictuosa (ilícita) del bien que adquiere o ayuda a negociar, pues de no ser así, estaríamos penalizando meras conductas imprudentes. Dicho así: el dolo del autor debe cubrir un conocimiento certero de que los bienes muebles que ingresan a su esfera de custodia, son de procedencia delictiva, sin necesidad de que ello suponga con exactitud cuál ha sido el delito cometido, así como sus circunstancias u otros pormenores".[90]

Por otro lado, el aprovechamiento está relacionado a la utilidad que el bien pueda otorgar al sujeto activo, siendo este un beneficio lucrativo.

---

[89] Fidel Rojas, *Jurisprudencia Penal y Procesal Penal*, (Lima: Idemsa 2000) 576.

[90] Raúl Peña Cabrera Freyre, *Delitos contra el Patrimonio – estudios de derecho penal parte especial*, 3ra edición, (Perú: Motivensa SRL, 2021) 287.

En cuanto a la determinación de la presunción del origen ilícito de los bienes, el juez, al momento de juzgar, no debe evaluar si el actor debía presumir, sino determinar si el actor presumió o no; por lo que Roy Freyre determina reglas para determinar dicha presunción:

1) Diferenciación entre el valor del bien en el mercado actual, con el precio con el que dicho bien fue comprado.
2) Incongruencia entre el valor del bien y la situación económica del vendedor o donante.
3) Escasa explicación razonable o nula de la forma en la que adquirió el bien, así como falta de documentación pertinente.[91]

La naturaleza dolosa de la receptación ha sido señalada por la jurisprudencia peruana a través de la Casación 186 - 2017 Ucayali en la que, en primer lugar, se desarrolla brevemente los requisitos del elemento subjetivo de la receptación en su modalidad básica:

DÉCIMOQUINTO: De otro lado, respecto al elemento subjetivo de la receptación, cabe reconocer que en su modalidad básica exige tres requisitos: a) Un elemento cognoscitivo normativo, consistente en obrar con conocimiento de un delito contra el patrimonio; b) Un elemento comisivo formulado de manera alternativa y que se predica de quien ayude a los responsables a aprovecharse de los efectos de ese delito o de quien reciba, adquiera u oculte tales efectos, que implica a su vez un elemento subjetivo de injusto: actuar con ánimo de lucro; y, c) Un elemento negativo, integrado por la circunstancia de que el sujeto activo no haya intervenido ni como autor ni como cómplice en el delito previo.

En segundo lugar, explica los tipos de dolo que pueden presentarse en el delito de receptación:

DÉCIMO SEXTO: Se trata de un delito eminentemente doloso, que puede ser sometido por dolo directo, con conocimiento certero de la procedencia ilícita de los bienes, como por dolo eventual, en los supuestos que el receptador se ha representado como razonablemente probable que tales bienes detenten origen en un delito de diversa naturaleza. En este último caso, el origen ilícito de los bienes receptados aparece con un alto grado de probabilidad, en virtud de las circunstancias coetáneas al hecho.

[91] Luis Roy Freyre, *Manual de Derecho penal. Parte especial*, (Lima: Eddili 1986), 143-145.

- **Agravantes del delito de receptación:**

Los agravantes son hechos que de forma negativa afectan la percepción del delito de receptación, tal como lo estipula el artículo 195 del Código Penal:

"La pena privativa de libertad será no menor de cuatro ni mayor de seis años y de sesenta a ciento cincuenta días-multa:

1. Si se trata de vehículos automotores, sus autopartes o accesorios.
2. Si se trata de equipos de informática, equipos de telecomunicación, sus componentes y periféricos.
3. Si la conducta recae sobre bienes que forman parte de la infraestructura o instalaciones de transporte de uso público, de sus equipos o elementos de seguridad, o de prestación de servicios públicos de saneamiento, electricidad o telecomunicaciones.
4. Si se trata de bienes de propiedad del Estado destinado al uso público, fines asistenciales o a programas de apoyo social.
5. Si se realiza en el comercio de bienes muebles al público.
6. Si se trata de gas, de hidrocarburos o de sus productos derivados.
7. Si la conducta recae sobre bienes que forman parte de la infraestructura o instalaciones públicas o privadas para la exploración, explotación, procesamiento, refinación, almacenamiento, transporte, distribución, comercialización o abastecimiento de gas, de hidrocarburos o de sus productos derivados, conforme a la legislación de la materia.

La pena será privativa de libertad no menor de seis ni mayor de doce años si se trata de bienes provenientes de la comisión de los delitos de robo agravado, secuestro, extorsión, trata de personas y trabajo forzoso".

En el caso del *ciberburrier* y su intervención dentro del delito de receptación, su comportamiento podría confundirse con el segundo de los agravantes mencionados en la norma, que hace referencia a los equipos de informática. Sin embargo, lo que el *ciberburrier* recibe es dinero en su cuenta bancaria a través de una transferencia electrónica, y no equipos de informática, como podrían ser computadoras, tablets, etc. Además, el *ciberburrier* no interviene en un delito consumado, el cual es un requisito para el delito de la receptación, sino que brinda un aporte esencial para que se produzca el delito de fraude informático.

3.4 El *ciberburrier* como autor del delito de lavado de activos

3.4.1. Conceptualización del delito de Lavado de activos

El autor Luis Sánchez precisa que "lavar dinero implica llevar al plano de la legalidad sumas monetarias que han sido obtenidas a través de operaciones ilícitas"[92]; es decir, consiste en brindar una apariencia de licitud a hechos en los que intervienen bienes o dinero de origen ilícito, tales como corrupción, secuestros y otros, para "poder disfrutar de los bienes sin despertar sospechas sobre su origen".[93]

Por otra parte, cabe señalar que el delito de lavado de activos es un fenómeno delictivo complejo porque cursa por un proceso conformado por fases por las que circula el valor patrimonial captado de forma ilícita: así, el dinero obtenido a través de un acto ilícito, revestido de "apariencia de legalidad mediante la realización de actividades económicas-comerciales para posteriormente ser ingresados o insertados en el circuito económico legal".[94]

El lavado de activos también es un delito transnacional, porque el proceso puede involucrar operaciones financieras en diversos países con el fin de perder el rastro del delito previo que dio origen a las ganancias ilegales.

Respecto al bien jurídico violentado, el Acuerdo Plenario 3-2010/CJ-116, en su fundamento jurídico 13, señala que es más compatible con la dinámica y finalidad de los actos de lavado de activos la presencia de una pluralidad de bienes jurídicos que son afectados o puesto en peligro de modo simultáneo o sucesivo, durante las etapas y operaciones delictivas que ejecuta el agente.

De la misma manera BLANCO CORDERO precisa que, al ocultarse bienes de origen delictivo, se produce un perjuicio a la operatividad de la administración de justicia y el orden socioeconómico. Asimismo, al tipificar el delito de lavado de activos se busca la estabilidad, orden, transparencia y legitimidad entre el sistema de justicia y el sistema económico financiero, evitando valerse de vacíos legales para que el hecho ilícito tenga apariencia de lícito, y eludiendo la función de incautar y decomisar el bien ilícito por parte del estado vulnerado.[95]

---

[92] Luis Sánchez Brot, *Lavado de dinero. Delito transnacional*, (Buenos Aires: La Ley. 2002),3.

[93] Isidoro Blanco Cordero, *El delito de blanqueo de capitales* (Pamplona: Thomson Reuters Aranzadi, 2012) 89.

[94] Shirley Muñico Patilla, "La lucha contra el lavado de activos: ¿estamos avanzando o retrocediendo? ¿realmente "nuestras autoridades están luchando contra la criminalidad"? ¿qué falta?»", *Revista.Ius.*et 1, n.º 1, (2018): 85 69 – 87.

[95] Blanco Cordero, *El delito de blanqueo de capitales*, 210-233.

En consecuencia, respecto al bien jurídico protegido en el delito de lavado de activos, me adhiero a la postura pluriofensiva, la cual señala que el delito de lavado de activos no afecta a un solo bien jurídico, sino que son varios los bienes jurídicos afectados en el delito de lavado de activos. De esta manera lo señala también el Tribunal Constitucional en su sentencia nro. 05811-PHC, en el fundamento número 10, al decir que los bienes jurídicos afectados en el lavado de activos son la credibilidad y transparencia del sistema financiero, la administración de justicia, la libre competencia, la estabilidad y seguridad del Estado y el sistema democrático.

Así pues, estos bienes jurídicos afectados pueden derivarse de un delito consumado, o de la tentativa de un delito, pero no de "(...)faltas o ilícitos no penales"[96]. Al referirme a la tentativa de un delito, podría ser el ejemplo del delito de sicariato, en el cual se entrega una cantidad de dinero al sicario para que mate a otra persona, sin embargo, suponiendo que este delito no llega a concretarse y queda en una tentativa, el dinero que recibió el sicario podría ya ser parte de un lavado de activos al insertarse al tráfico económico o por simplemente recibirlo, como señala la modalidad típica de ocultamiento y tenencia del delito de lavado de activos.

Podría considerarse la posibilidad de que la conducta del *ciberburrier* configure este delito en la medida en que sus actos conciernen precisamente a la transferencia de activos monetarios por medio de cuentas bancarias y otros instrumentos informáticos. En tal sentido, guarda semejanzas con conductas paradigmáticas que constituyen lavado de activos, como el depósito de dinero en efectivo de origen delictivo en una cuenta bancaria, insertándolo así en el tráfico de bienes ordinario.

3.4.2. Regulación del delito de lavado de activos en el Estado Peruano y análisis del tipo penal

Es pertinente resaltar que, en un inicio, el delito de lavado de activos tenía como finalidad la persecución del tráfico ilícito de drogas. Luego la legislación nacional fue evolucionando y se vio influenciada por tratados internacionales, como la Convención de las Naciones Unidas contra el Tráfico Ilícito de Estupefacientes y Sustancias Sicotrópicas (Convención de Viena de 1988) y por la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional (Convención de Palermo del 2000), así como también hay influencia del Grupo de Acción Financiera Internacional (GAFI), con sus 40 recomendaciones.

[96] Percy García Cavero, *Derecho Penal Económico*, (Lima: Instituto pacifico, 2015), 576.

En el Perú, la configuración típica del delito de lavado de activos está determinada por el Decreto Legislativo N° 1106, de fecha 19 de abril del 2012, denominado Decreto Legislativo de Lucha eficaz contra el lavado de activos y otros delitos relacionados a la minería ilegal y crimen organizado. Como hemos mencionado en el primer capítulo, la presente tesis tiene un enfoque de investigación en el cual prevalece la parte dogmática sobre la procesal, por lo que analizaremos sólo los artículos que se relacionan con la intervención del *ciberburrier*, que son los siguientes: artículo 1°, Actos de conversión y transferencia; artículo 2°, Actos de nacional de dinero o títulos valores de origen ilícito; y el artículo 10°, Autonomía del delito y prueba indiciaria.

> **Artículo 1°, Actos de conversión y transferencia**: El que convierte o transfiere dinero, bienes, efectos o ganancias cuyo origen ilícito conoce o debía presumir, con la finalidad de evitar la identificación de su origen, su incautación o decomiso, será reprimido con pena privativa de la libertad no menor de ocho ni mayor de quince años y con ciento veinte a trescientos cincuenta días multas.

En el mencionado artículo, como ya se señaló anteriormente, se observan conductas que encajan con el comportamiento del *ciberburrier*, en el sentido que recibe en su cuenta bancaria dinero para luego transferirlo a la cuenta que le indique el tercero. El tipo penal menciona que el agente conoce o debía presumir el origen ilícito de este dinero, por lo que, desde mi punto de vista, en este artículo el *ciberburrier* sería un cómplice primario, ya que su participación en el delito de lavado de activos es imprescindible, al necesitar el autor del delito de lavado de activos una persona que reciba el dinero en su cuenta bancaria para luego realizar la transferencia a otra cuenta señalada por el autor. Por lo tanto, será trabajo del Ministerio Público probar que el *ciberburrier* conocía o debía presumir que el dinero que recibió en su cuenta tenía un origen delictivo para luego transferirlo, además de probar que la finalidad de esta transferencia era evitar la identificación de su origen.

Posteriormente, el 26 de noviembre del 2016 se publicó el Decreto Legislativo N°1249, que en su artículo 5° modifica los artículos 2°, 3° y 10° del DL N° 1106. De esta manera, actualmente los mencionados artículos están redactados de la siguiente manera:

> **Artículo 2.- Actos de ocultamiento y tenencia**
>
> El que adquiere, utiliza, posee, guarda, administra, custodia, recibe, oculta o mantiene en su poder dinero, bienes, efectos o ganancias, cuyo origen ilícito conoce o debía presumir, será reprimido con pena privativa de la libertad no menor de ocho ni mayor de quince años y con ciento veinte a trescientos cincuenta días multa.

Articulo 3.- Transporte, traslado, ingreso o salida por territorio nacional de dinero o títulos valores de origen ilícito

El que transporta o traslada consigo o por cualquier medio dentro del territorio nacional dinero en efectivo o instrumentos financieros negociables emitidos "al portador" cuyo origen ilícito conoce o debía presumir, con la finalidad de evitar la identificación de su origen, su incautación o decomiso; o hace ingresar o salir del país consigo o por cualquier medio tales bienes, cuyo origen ilícito conoce o debía presumir, con igual finalidad, será reprimido con pena privativa de la libertad no menor de ocho ni mayor de quince años y con ciento veinte a trescientos cincuenta días multa.

Articulo 10.- Autonomía del delito y prueba indiciaria

El lavado de activos es un delito autónomo por lo que para su investigación, procesamiento y sanción no es necesario que las actividades criminales que produjeron el dinero, los bienes, efectos o ganancias, hayan sido descubiertas, se encuentren sometidas a investigación, proceso judicial o hayan sido previamente objeto de prueba o condena.

El conocimiento del origen ilícito que tiene o que debía presumir el agente de los delitos que contempla el presente Decreto Legislativo, corresponde a actividades criminales como los delitos de minería ilegal, el tráfico ilícito de drogas, el terrorismo, el financiamiento del terrorismo, los delitos contra la administración pública, el secuestro, el proxenetismo, la trata de personas, el tráfico ilícito de armas, tráfico ilícito de migrantes, los delitos tributarios, la extorsión, el robo, los delitos aduaneros o cualquier otro con capacidad de generar ganancias ilegales, con excepción de los actos contemplados en el artículo 194 ° del Código Penal. El origen ilícito que conoce o debía presumir el agente del delito podrá inferirse de los indicios concurrentes en cada caso.

Para los fines el presente trabajo, resulta pertinente mencionar cuáles fueron los cambios en los artículos 2°,3° y 10° del DL N° 1106.

Respecto al artículo 2°se agregó la palabra “posee” y se eliminó la parte que hace referencia a un elemento subjetivo distinto del dolo, como es el elemento de tendencia interna trascendente; es decir, se eliminó “la finalidad de evitar la identificación de su origen, su incautación o decomiso”. Ante estas modificaciones, cabe manifestar que el legislador convierte este artículo en un tipo penal parecido al de la receptación, al mencionar que el agente “adquiere, utiliza, guarda, posee, administra, custodia, recibe, oculta o mantiene en su poder”,

pues se configuraría el tipo penal con el simple hecho de recibir o tener la posesión del dinero o las ganancias de origen ilícito. Asimismo, el tipo penal se refiere al dolo eventual cuando señala que el agente conoce o debía presumir, lo cual significa que el agente debe estar en capacidad de poder representarse el elevado riesgo de la procedencia delictuosa y poder diferenciarla de una conducta socialmente permitida.

En el caso del *ciberburrier*, se observa que cumpliría la modalidad típica de ocultamiento y tenencia, ya que el *ciberburrier* recibe el dinero en su cuenta bancaria y se encarga de transferirlo a la cuenta que le ha indicado el autor del delito de fraude informático. Ahora bien, el tipo penal del fraude informático no indica el tiempo que tiene el *ciberburrier* el dinero en su cuenta bancaria; empero, el sentido común nos indica que se trataría de un tiempo corto, en vista de que el *ciberburrier* debería recibir un pago por esta operación económica. Asimismo, podría darse el caso de que, por algún motivo, el *ciberburrier* no logre reenviar este dinero a la cuenta que le indica el autor del delito de fraude informático, configurándose de esta manera la modalidad típica de ocultamiento y tenencia.

En cuanto al artículo 3°, se sustituyó la referencia a "títulos valores" por "instrumentos financieros negociables emitidos al portador". La presente disposición alude a la característica de transnacionalidad del delito de lavado de activos, puesto que el lavado puede incluir a varios países, con la finalidad de dificultar el rastro del dinero. Aquí, no cabría una imputación al *ciberburrier* como autor por el delito de lavado de activos bajo la modalidad típica de transporte, en vista de que el artículo, además de hacer referencia a cualquier instrumento financiero, también señala que el agente hace ingresar o salir del país, por cualquier medio, bienes o dinero en efectivo cuyo origen ilícito conoce o debía presumir. Y en el caso del *ciberburrier*, su conducta consiste en reenviar dinero, pero a través de transferencias bancarias vía internet, por lo que no se estaría configurando esta modalidad.

En lo concerniente al artículo 10°, se observa que, a la lista de actividades cuyo origen ilícito el agente del delito de lavado de activos conoce o debía presumir, se añade el "financiamiento del terrorismo". La primera parte de esta disposición hace referencia a la parte procesal, cuando menciona que el delito de lavado de activos es un delito autónomo, pues señala que no es necesario que, para la investigación, procesamiento y sanción de las actividades criminales que dieron lugar al lavado de activos, estas se hayan probado.

Sin embargo, considero que el artículo 10 se refiere a un estándar de convicción mínimo, también llamado sospecha inicial simple, el cual se aplica en las diligencias preliminares. Tal como se acordó en el Pleno Casatorio 1-2017/CIJ-433 en el fundamento 29, el estándar o grado de convicción no es el mismo durante el desarrollo de la actividad procesal o del procedimiento

penal: la ley fija esos niveles de conocimiento, varía progresivamente en intensidad. Seguidamente, se hace la diferenciación en el inciso F. Para iniciar diligencias preliminares solo se exige elementos de convicción que sostengan una "sospecha inicial simple"; para formalizar la investigación preparatoria se necesita "sospecha reveladora"; para acusar y dictar el auto de enjuiciamiento se precisa "sospecha suficiente"; y para proferir auto de prisión preventiva se demanda "sospecha grave"—la sospecha más fuerte en momentos anteriores al pronunciamiento de una sentencia. La sentencia condenatoria requiere elementos de prueba más allá de toda duda razonable.

Con respecto al segundo párrafo del artículo 10°, se menciona que el agente conoce o debía presumir que el origen ilícito del dinero corresponde a actividades criminales, y se procede a enunciar una lista de delitos, para concluir diciendo que puede ser cualquier otro delito con capacidad de generar ganancias ilegales. Como hemos revisado anteriormente, fueron tratados internacionales los que buscaron luchar contra el delito de lavado de activos, como la Convención de Palermo, que en su artículo 6.2.b recomienda que, para la configuración del delito de lavado de activos, los activos o capitales provengan de delitos graves. A pesar de esto, en el Perú, a través del Pleno Casatorio N° 1-2017/CIJ-433, se ha determinado lo siguiente:

> 16.° Por consiguiente, es de concluir destacando lo innecesario e inconveniente, para un estándar de eficacia de las políticas nacionales, regionales e internacionales de prevención y represión penal del delito de lavado de activos, desarrollar nociones de gravedad que perjudican la útil y adecuada regulación actual del artículo 10 del Decreto Legislativo 1106, la misma que involucra toda actividad criminal capaz de producir ganancias ilegales. Además, cabe precisar que el único criterio de gravedad que ha formalizado la legislación penal vigente en el Perú, para habilitar la persecución, procesamiento y sanción de las conductas que constituyen delito de lavado de activos, se refiere al monto relevante del valor económico de la operación de colocación, intercalación o integración realizada por el agente, y que es considerado como circunstancia agravante específica en al artículo 4, inciso 3, del Decreto Legislativo 1106, cuando dicho monto excede el equivalente a más de quinientas Unidades Impositivas Tributarias.

Desde mi punto de vista, el Estado peruano debió tipificar una lista cerrada mencionando cuáles son los delitos que pueden dar origen al lavado de activos, pues cuando el

artículo 10° señala que puede ser cualquier otro delito con capacidad de generar ganancias ilegales, deja abierta las interpretaciones para imputar el delito de lavado de activos, como podría ser la conducta del *ciberburrier*. Además, se deberían ampliar los criterios para determinar la gravedad en el delito previo, y así establecer un filtro importante para la imputación e interpretación del delito de lavado de activos.

- **Tipicidad del delito, objetiva y subjetiva**

Elemento objetivo:

El sujeto activo en el delito de lavado de activos es la persona que realiza las acciones que se describen en las modalidades típicas, que son los siguientes: conversión y transferencia, ocultación y tenencia, transporte y traslado. Este delito puede realizarse también por la misma persona que ejecutó la actividad criminal previa, en el caso del denominado autolavado. Cabe mencionar que el delito de lavado de activos también puede ser cometido por omisión, tal como lo señala el artículo 5° del Decreto Legislativo N° 1106: Omisión de comunicación de operaciones o transacciones sospechosas. Es pues un delito común que no tiene una condición especial para su comisión. A pesar de esto, el delito de lavado de activos tiene supuestos agravados en los que se toma en consideración la situación del sujeto activo. Es así que, el artículo 4° del Decreto Legislativo N° 1106 agrava la sanción del delito cuando el autor es funcionario público o miembro de una organización criminal.

El sujeto pasivo es el Estado, al evitarse que el sector público cumpla sus labores de acreencias mediante la incautación o decomiso, cesando el tráfico ilícito de los bienes obtenidos mediante estas acciones ilegales. También se genera un perjuicio al sector económico vulnerando la libre competencia.

Como hemos revisado, el delito de lavado de activos implica un conjunto de operaciones para que el autor del delito pueda ocultar la procedencia delictiva del dinero o los bienes y luego buscar integrarlos en el sistema económico y financiero. Cabral agrega que, para completar la acción que desemboca en el delito de lavado de activos, este debe cursar por un proceso, por el cual los valores patrimoniales involucrados en el sistema económico legal son de libre disposición para la transformación, cambiando de estatus de la forma en la que se obtuvo.[97]

[97] Cristian Javier Cabral, *Delito de lavado de dinero. Antecedentes internacionales, relación con el terrorismo y medio de desarrollo, Delitos Económicos*, (Argentina: Editorial Ministerio de Justicia y Derechos Humanos de la Nación, 2013),336.

Este proceso es desglosado en tres fases para su consumación, las cuales pueden realizarse de forma separada o simultáneamente. Primero, la colocación, fase en la cual el dinero ilícito se toma para brindarle apariencia de haber sido obtenido de forma legal. En segundo lugar, la transformación, en la cual el dinero es conducido a su destino final como si se tratara de un elemento lícito, en beneficio del sujeto activo del delito, haciendo menos evidente el desbalance financiero. Finalmente, la integración: fase en la que el dinero ilícito se convierte en lícito y puede ser de fácil circulación en el sistema financiero, en adelante cumpliendo fines lícitos.

Respecto al objeto material del delito, se debe tomar en cuenta los bienes sobre los que recaerá la conducta típica: ganancias en bienes o dinero, o propiamente efectos positivos que beneficien al autor. Como los bienes derivan de un origen ilícito, el delito de lavado de activos conecta con otro delito y, de no encontrarse presente, no existiría objeto idóneo para el delito.[98]

Elemento subjetivo:

El delito de lavado de activos es un delito complejo, puesto que dependerá de la modalidad de su ejecución la determinación de si es un delito doloso y de resultado, como hemos visto en los artículos 1,2,3 y 10 del DL N°1106. En principio se trataría de un delito doloso, ya que se realiza mediante acciones premeditadas, con el fin de brindar la apariencia de licitud a un beneficio que se obtuvo de manera ilícita y que para su configuración se requiere que el agente actúe con conocimiento o presunción de conocimiento de que está lavando dinero de procedencia delictiva, con la intención de evitar que la justicia pueda identificar, incautar o decomisar ese dinero ilícito.

Como ya se ha analizado, también se aprecia en el DL N°1106, en los artículos 1° (actos de conversión y transferencia) y 3° (transporte y traslado), un elemento subjetivo distinto del dolo, que es el elemento de tendencia interna trascendente. Este elemento requiere obrar con el ánimo, finalidad o intención adicional de lograr un resultado o una ulterior actividad, distintos a la realización del tipo. En el caso del lavado de activos, el elemento de tendencia interna trascendente es la finalidad de evitar la identificación del origen, incautación o decomiso de los bienes, efectos o ganancias cuyo origen ilícito conoce el agente o debía presumir.

En los elementos subjetivos del dolo, soy de la opinión de que el legislador quiere restringir el ámbito de punición propia del tipo doloso, incorporando en la descripción típica algún elemento subjetivo especial o un propósito especial, que sería el elemento de tendencia

[98] Blanco Cordero, *El delito de blanqueo de capitales*, 246.

interna trascendente. Este elemento, como vimos en los artículos 1° y 3° del Decreto Legislativo N ° 1106, tiene la finalidad de evitar la identificación de su origen, incautación o decomiso.

Asimismo, en el tipo penal se observa que esta finalidad o ánimo no necesita ser realizada para la consumación, por lo que se puede concluir que, en estos artículos, el delito de lavado de activos sería uno de peligro abstracto. Como ha señalado García Cavero: "los delitos de peligro abstracto se caracterizan por sancionar comportamientos peligrosos sin que efectivamente se hayan puesto en peligro o lesionado un objeto que representa al bien jurídico. Es la peligrosidad de la conducta lo que sustenta su incriminación penal."[99]

Por lo tanto, el delito de lavado de activos se consuma con la realización de la conducta típica, y no es necesaria la identificación de las actividades criminales que dieron origen al dinero o bienes.

Por otra parte, respecto a la tentativa, esta podría producirse en los casos que la modalidad del delito de lavado de activos (conversión, ocultamiento y transporte) permita una ejecución parcial que tenga suficiente sentido delictivo. Por ejemplo, respecto al artículo 1°, sobre actos de conversión y transferencia, y al artículo 3°, sobre transporte, traslado, ingreso o salida por territorio nacional de dinero o títulos valores de origen ilícito; hemos analizado que cuentan con el elemento de tendencia trascendente, que presentan la estructura de delitos de peligro abstracto. Sin embargo, en estas modalidades, el delito se consuma con las conductas típicas de convertir o transferir, transportar o trasladar, por lo que no es necesario que se observe la finalidad de evitar la identificación del origen delictivo del bien o su incautación o decomiso.

Respecto al artículo 2°, relacionado a actos de ocultamiento y tenencia, el Acuerdo Plenario 3-2010/CJ-116 de la Corte Suprema de Justicia del Perú ha señalado lo siguiente en su fundamento jurídico 16°:

> "En lo concerniente a los actos que tipifica el artículo 2° como supuestos de ocultamiento y tenencia, su estructura ejecutiva es la propia de los delitos permanentes. En ellas, pues, las posibilidades delictivas incluidas imponen que el momento consumativo y la producción del estado antijurídico generado por la conducta realizada se mantenga en el tiempo por voluntad expresa o implícita del agente. La permanencia del estado antijurídico, pues, y por consiguiente de la consumación durará lo que el agente decida o lo que este logre mantener sin que las agencias de control descubran o detecten la procedencia ilícita o lo ficticio de la apariencia de legalidad de los activos.

[99] García Cavero, *Derecho Penal Parte General*, 454.

> La necesidad de distinguir la condición instantánea o permanente de la consumación en los actos que constituyen delitos de lavado de activos, adquiere importancia práctica para resolver problemas relacionados con la prescripción de la acción penal o con las posibilidades de una participación post consumativa".

Por otro lado, es preciso señalar que, la configuración típica del delito de lavado de activos viene establecida por el ordenamiento jurídico de cada país. En la legislación peruana es necesario recordar para el análisis del delito, el principio de legalidad (artículo II, del Título Preliminar del Código Penal Peruano) el cual señala que nadie será sancionado por un acto no previsto como delito o falta por la ley vigente al momento de su comisión, ni sometido a pena o medida de seguridad que no se encuentren establecidas en ella. Es por ello que, para determinar si un hecho califica o no como delito de lavado de activos, deberá revisarse la norma penal; esto es, el Decreto Legislativo 1106.

Es pertinente mencionar este principio, en vista que los Estados han regulado de manera distinta el delito de lavado de activos. Sobre el particular, en el derecho comparado observamos que, en España por ejemplo, se admite la modalidad culposa del delito de blanqueo de capitales.

En esa misma línea, al imputarse el lavado de activos, si es que no se trata de un autolavado, se debe conocer o presumir de la comisión de otro delito previo del cual se origina el beneficio, tomando en cuenta que también podría solo conocer el riesgo elevado, al cual se encuentra o se encontró supeditado para la obtención del mismo; es decir, que haya procedido de una actividad delictiva.

De ese modo, la Casación 92-2017-Arequipa determina que el delito fuente es un elemento de carácter normativo del tipo objetivo; por lo tanto, para que una conducta sea típica, debe reunir todos los elementos normativos y descriptivos del tipo. Si falta uno de ellos, la conducta deviene en atípica. Así pues, el delito fuente del lavado de activos debe estar taxativamente determinado por la Ley. Para ser un delito fuente se requiere de los siguientes factores:

- *Descripción del suceso fáctico, mencionando el presunto autor o participe, indicando fecha y lugar en el que ocurrió.*
- *Conocimiento o presunción del mismo del agente sobre el delito previo.*
- *Capacidad para generar ganancias ilegales.*
- *Gravedad del delito.*

- **Agravantes y atenuantes del delito de lavado de activos:**

Los agravantes y atenuantes se encuentran regulados en el artículo 4 del Decreto Legislativo 1106:

Artículo 4º.- Circunstancias agravantes y atenuantes

La pena será privativa de la libertad no menor de diez ni mayor de veinte años y trescientos sesenta y cinco a setecientos treinta días multa, cuando:

1. El agente utilice o se sirva de su condición de funcionario público o de agente del sector inmobiliario, financiero, bancario o bursátil.
2. El agente cometa el delito en calidad de integrante de una organización criminal.
3. El valor del dinero, bienes, efectos o ganancias involucrados sea superior al equivalente a quinientas (500) Unidades Impositivas Tributarias.

La pena será privativa de la libertad no menor de veinticinco años cuando el dinero, bienes, efectos o ganancias provienen de la minería ilegal, tráfico ilícito de drogas, terrorismo, secuestro, extorsión o trata de personas.

En el caso de los atenuantes del delito de lavado de activos, se genera que el delito ya no sea valorado de manera excesiva, estableciéndose que la pena privativa de la libertad será no menor de cuatro ni mayor de seis años y de ochenta a ciento diez días multa, cuando el valor del dinero, bienes, efectos o ganancias involucrados no sea superior al equivalente a cinco (5) Unidades Impositivas Tributarias.

La misma pena se aplicará a quien proporcione a las autoridades información eficaz para evitar la consumación del delito, identificar y capturar a sus autores o partícipes, así como detectar o incautar los activos objeto de los actos descritos en los artículos 1º, 2º y 3º del presente Decreto Legislativo.

3.5 El *ciberburrier* y la posibilidad del concurso de delitos

A lo largo de la presente tesis, se ha analizado el comportamiento del *ciberburrier* en los delitos de fraude informático, receptación y lavado de activos. Como hemos visto, existen importantes similitudes con este último, mientras que, en el caso de la receptación existe una diferencia crucial en la tipicidad objetiva. Según lo revisado anteriormente, se ha evidenciado

que el delito de receptación no encaja en el tipo penal de fraude informático, puesto que aquel delito tiene como requisito que los bienes provengan de un delito consumado.

Sin embargo, debemos analizar la posibilidad de que el agente, con su conducta, configure tanto un fraude informático como un lavado de activos, por lo que se revisará el eventual concurso de delitos en el que se encontraría el *ciberburrier* con su comportamiento.

La posibilidad de que nos encontremos frente al concurso de delitos se da "(...)cuando una misma persona aparece como autor de varios delitos independientes entre sí o cuando su conducta se adecúa a dos o más tipos legales(...)"[100]. A partir de ello, debe diferenciarse entre concurso ideal y concurso real de delitos.

El concurso real de delitos se da cuando existen diversos hechos realizados por un mismo sujeto, configurándose distintos delitos imputados a un solo autor. Sanz Morán precisa que el concurso real se caracteriza por la existencia de la pluralidad de infracciones, que provienen de tantas acciones independientes, por un mismo autor.[101]

En contraste, según ORTS, "el concurso ideal supone una unidad de hecho y una pluralidad de infracciones".[102] En otras palabras, se trata de una sola acción—un solo hecho—pero que puede subsumirse dentro de diferentes tipos penales.

En el caso bajo análisis, se produciría un concurso real de delitos solo si el *ciberburrier* realiza distintas acciones. Ello, sin embargo, no es el caso. Como hemos revisado, la función del *ciberburrier* se cumple mediante la recepción y envío del dinero. Podría argumentarse que son dos acciones que realiza el *ciberburrier*: recibir el dinero en su cuenta bancaria y enviarlo a otra cuenta. Sin embargo, consideradas de forma independiente la una de la otra, vemos que la primera no puede configurar ningún tipo delictivo pues, como se señaló, la receptación implica la previa consumación de un delito. En otras palabras, no existe la posibilidad de concurso real entre los tipos penales considerados dada la conducta del *ciberburrier*.

Ahora bien, recibir y enviar dinero mediante transferencia bancaria a cambio de una comisión sí puede enmarcarse dentro de los delitos de lavado de activos y fraude informático. Pienso que esta posibilidad se manifiesta especialmente en las modalidades típicas de lavado de activos en sus artículos 1° (actos de conversión y transferencia); y 2° (actos de ocultamiento

---

[100] Villavicencio, *Derecho penal básico*, 2019, 125.

[101] Angel José Sanz Morán, *El concurso de delitos en la reforma penal*, (Madrid: Consejo General del Poder Judicial, 1995) 227.

[102] Enrique Orts Berenguer, José Luis Gonzáles Cussac, *Compendio de Derecho Penal Parte General*, (Valencia: Tirant lo blanch,2019) 485.

y tenencia). En ambos casos puede hablarse tanto de un origen delictivo y como de una inserción de los bienes en el tráfico ordinario. Dado que no existe una lista cerrada de delitos de origen para los bienes en el caso del lavado de activos, esta posibilidad permanece vigente.

Frente a esta posibilidad, se genera la siguiente alternativa. Por un lado, puede aplicarse el principio de consunción, el cual nos dice que hay preceptos penales que tienen una regulación más amplia que engloba a varias conductas; es decir, una regulación que protege a varios bienes jurídicos, o también llamados delitos pluriofensivos.

Sin embargo, hay un requisito para que se produzca esta absorción: que el agente haya hecho todo orientado hacia la finalidad principal. Este último requisito es problemático, puesto que el Ministerio Público deberá establecer si el *ciberburrier* tenía conocimiento de que su intervención servía para consumar un delito de fraude informático o tenía la finalidad de una complicidad en el delito de lavado de activos.

En la práctica, considero que la respuesta a este problema, se encontraría en la conducta del *ciberburrier* al recibir y reenviar dinero, ya que encaja mejor en el delito de lavado de activos. Esta postura la respaldo por la cláusula general que tiene el artículo 10° del DL N° 1106 de lucha eficaz contra el lavado de activos y otros delitos relacionados a la minería ilegal y crimen organizado, el cual señala que el conocimiento del origen ilícito que tiene o que debía presumir el agente corresponde a una lista de actividades criminales como son los delitos de minería ilegal, tráfico ilícito de drogas, terrorismo, etc, para concluir señalando, que puede ser cualquier otro con capacidad de generar ganancias ilegales.

En ese sentido, es difícil determinar que el *ciberburrier* conoce que su conducta contribuye a facilitar el delito de fraude informático, puesto que tendría que probarse que sabe que el dinero que recibe y debe reenviar proviene de la manipulación o interferencia del funcionamiento de un sistema informático, por ello considero que el comportamiento del *ciberburrier* se adecúa más al de la cláusula general del artículo 10° del DL N°1106, pues este exige que el agente tenga el conocimiento o deba presumir que el origen ilícito del dinero, bienes, efectos o ganancias provengan de cualquier otro delito con capacidad de generar ganancias ilegales.

La segunda opción sería aplicar el principio de alternatividad, el cual hace referencia a dos normas específicas que calzan en el mismo hecho. Por ello se debe elegir el delito que tiene la pena más grave, con el que se regula el bien jurídico más importante, lo que se denomina un concurso de normas. Sin embargo, este principio viene de la doctrina española, y además cuenta con una norma en el código penal español, situación que no pasa en el código penal peruano. En mi opinión, el principio que resuelve mejor la intervención del *ciberburrier* en el delito de

fraude informático y el delito de lavado de activos, es el principio de asperación o exasperación que señala el código penal peruano en su artículo 48°:

Cuando varias disposiciones son aplicables al mismo hecho se reprimirá hasta con el máximo de la pena más grave, pudiendo incrementarse ésta hasta una cuarta parte, sin que en ningún caso pueda exceder de treinta y cinco años.

Cada caso que se presente tendrá sus propias características, pero pienso que el *ciberburrier* estaría inmerso tanto en el delito de fraude informático como en el de lavado de activos, generándose un concurso ideal de delitos, siendo el delito más grave el de lavado de activos, el cual tiene una pena base que oscila entre los 8 y 15 años de cárcel.

3.6 La responsabilidad penal del *ciberburrier*: postura personal

Finalmente, articularé aquí mi punto de vista sobre la responsabilidad penal del *ciberburrier* en el delito de fraude informático. Como he mencionado anteriormente, el autor del delito de fraude informático necesita el apoyo de un intermediario, al que se denomina "*ciberburrier*", para que reciba las transferencias de dinero no autorizadas y las reenvíe a la cuenta que el autor del delito de fraude informático le indicará, todo ello a cambio de una comisión.

La conducta del *ciberburrier* en estos casos se adecúa al tipo penal de fraude informático, pues resulta evidente que su intervención es imprescindible para obtener el provecho ilícito en perjuicio del titular de la cuenta bancaria. Este aspecto debe resaltarse porque se descartaría así que se trate de un acto post consumativo, lo cual evita, a su vez, la imputación a título de cómplice, y hace imposible la aplicación del tipo penal de receptación.

A pesar de ello, para que la conducta del *ciberburrier* pueda adecuarse a la participación como cómplice del delito de fraude informático, no es suficiente imputar que su conducta constituye una ayuda o auxilio al hecho punible (el aspecto objetivo), sino que también deberá poder atribuirse el aspecto subjetivo de la complicidad (dolo). En cuanto a este, suscribo la teoría cognitiva del dolo, la cual se enfoca en la imputación que se hace del conocimiento que tiene el cómplice acerca del significado de sus actos, lo que implicaría que el *ciberburrier* conoce que su comportamiento de recibir y reenviar dinero a cambio de una comisión sirve para integrarse o facilitar un proyecto delictivo. Surge de esta manera la interrogante acerca de cómo se determina este conocimiento. Es aquí donde un sector de la doctrina apela a la prueba por indicios.

La prueba indiciaria tiene exigencias a nivel jurisprudencial, pero también están las exigencias legales. Así pues, el Código Procesal Penal peruano, en cuanto a la valoración de la

prueba que debe tener el Juez, exige en el artículo 158 inciso 3, que la prueba por indicios requiere:

a) que el indicio esté probado b) que la inferencia esté basada en las reglas de la lógica, la ciencia o la experiencia c) que cuando se trate de indicios contingentes, éstos sean plurales, concordantes y convergentes, así como que no se presenten contraindicios consistentes.

En esa misma línea el Tribunal Constitucional en su sentencia expediente N°728-2008-PHC-TC Lima (caso Giuliana Llamoja) en su fundamento N°27 ha señalado que:

> "Asimismo, cabe recordar que el razonamiento probatorio indirecto, en su dimensión probatoria, exige que la conclusión sea adecuada, esto es, que entre los indicios y la conclusión exista una regla de la lógica, máxima de la experiencia o conocimiento científico, y que, como dijimos supra, el razonamiento esté debidamente explicitado y reseñado en la sentencia.
>
> El órgano jurisdiccional debe explicitar el razonamiento a través del cual, partiendo de los indicios, ha llegado la convicción de la existencia del hecho delictivo y la participación del imputado, con el objeto de garantizar hasta el límite de lo posible la racionalidad de su decisión (examen de suficiencia mínima)".

Mediante la prueba por indicios sería posible determinar en el proceso penal que el *ciberburrier*, con su comportamiento, facilitaba un delito, puesto que brinda su cuenta bancaria para recibir un dinero y luego lo reenvía a cambio del pago de una comisión, pero no sucede lo mismo con la imputación del conocimiento exacto del origen de las transferencias dinerarias.

Estos aspectos de la prueba indiciaria colisionan con el doble dolo del cómplice que se suele exigir en estos escenarios delictivos. En primer lugar, se deberá probar que el *ciberburrier* tenía conocimiento que recibía un dinero en su cuenta bancaria; o sea, que había un acuerdo con la persona que le envió el dinero para después reenviarlo a la cuenta de un tercero a cambio del pago por la intermediación. Considero que este aspecto sería viable de probar con el levantamiento del secreto bancario y el de las comunicaciones.

En segundo lugar, se deberá probar que el *ciberburrier*, como cómplice, conocía los elementos esenciales del fraude informático; es decir, que debería saber de dónde proviene este dinero que recibe en su cuenta bancaria para después reenviarlo, así como el sujeto pasivo del delito de fraude informático. Es este último aspecto el que resulta difícil de probar.

El Código Penal peruano señala que la complicidad debe ser dolosa, pues el cómplice debe tener conocimiento de que su comportamiento sirve para auxiliar o favorecer un delito. Si bien eso es cierto, el Juez puede recurrir a las máximas de la experiencia y argumentar que el cibeburrier podía concebir que la operación que realiza tiene un trasfondo delictivo: primero, porque es una operación de transferencia bancaria vía internet, fácil de realizar, pues brinda su número de cuenta bancaria para recibir un dinero; y segundo, porque a cambio de ello recibirá una comisión. Sin embargo, esto no significa que el *ciberburrier* conozca con certeza que el dinero que recibe y reenvía proviene del delito de fraude informático.

Es por ello que soy de la opinión de que el *ciberburrier*, en principio, no puede ser un cómplice en el delito de fraude informático, porque no se puede contar con los indicios suficientes para imputar ese conocimiento acerca de la procedencia del dinero que recibe y reenvía, salvo que se pueda demostrar en el proceso penal mediante alguna prueba, ya sean correos o mensajes, etc, que el *ciberburrier* tenía conocimiento del delito de fraude informático en el cual participaba.

Entonces, según lo explicado hasta este punto, el *ciberburrier* no puede tener una responsabilidad como cómplice en el delito de fraude informático, por lo que procederé a proponer una respuesta acerca de cuál pienso sería la responsabilidad penal del *ciberburrier* por su intermediación, ya sea a título de autor o cómplice de algún delito.

Dada la complejidad del caso, se analizó la relación que podría tener el *ciberburrier* con el delito de lavado de activos. En primer término, porque, en la actualidad, para este delito se exige que el dinero o los bienes provengan de cualquier actividad criminal con capacidad de generar ganancias ilegales, y, en segundo término, porque el lavado de activos puede ser imputado a las personas que intervinieron en el delito previo (autolavado). En el contexto del fraude informático, al *ciberburrier* no se le puede imputar el conocimiento exacto del origen del dinero que se le envía a su cuenta para ser reenviado, pero sí que provenía de una actividad criminal en función de los indicios, como son la cantidad de dinero que el *ciberburrier* recibe y reenvía a otras cuentas bancarias y, además, las altas comisiones que cobra por su función.

Por tanto, tiene sentido que al *ciberburrier*, en este último aspecto, se le pueda imputar la autoría en el delito de lavado de activos. Ahora bien, las modalidades típicas del delito de lavado de activos que hemos revisado son tres: actos de conversión y transferencia, actos de ocultamiento y tenencia, y finalmente el transporte y traslado. La modalidad de actos de conversión y transferencia es la que mejor calza con el comportamiento del *ciberburrier*, puesto que esta modalidad señala que: el que convierte o transfiere dinero, bienes, efectos o ganancias

cuyo origen ilícito conoce o debía presumir, con la finalidad de evitar la identificación de su origen, su incautación o decomiso. De aquí se puede observar que esta modalidad se concreta con el comportamiento de convertir o transferir, acción que realiza el *ciberburrier* y que se ve respaldada por la parte que hace referencia al dolo eventual, cuando señala: "cuyo origen ilícito conoce o debía presumir". En relación al elemento de tendencia trascendente, como es la finalidad de evitar la identificación del origen delictivo, la incautación o decomiso, ya se analizó y se determinó que no es un requisito indispensable para imputar esta modalidad, pues basta la conducta típica de convertir y transferir.

Luego está la modalidad de ocultamiento y tenencia, la cual tiene una estructura parecida al delito de receptación, pues señala que "el que adquiere, utiliza, posee, guarda, administra, custodia, recibe, oculta o mantiene en su poder dinero, bienes, efectos o ganancias, cuyo origen ilícito conoce o debía presumir". En otras palabras, esta modalidad se concretaría con el simple hecho de recibir un bien o dinero con origen ilícito, pues a diferencia de los actos de conversión y transferencia, y los actos de transporte y traslado, no cuenta con el elemento de tendencia trascendente. Desde mi punto de vista, es una deficiente técnica legislativa, puesto que implicaría la posibilidad, mediante una interpretación literal de la norma, de imputar el delito de lavado de activos a la receptación de cualquier bien o cantidad de dinero; por ejemplo, un reloj, un equipo de sonido o mil soles. Podría presentarse una modalidad de ocultamiento y tenencia si es que el *ciberburrier* recibe el dinero en su cuenta bancaria pero por algún motivo no llega a reenviarlo.

Finalmente, la tercera modalidad del lavado de activos, como se revisó, quedó descartada para el análisis de la intervención del *ciberburrier*, ya que hace referencia al traslado de dinero en efectivo, y no es el caso de la transferencia que realiza el *ciberburrier*, la cual se realiza vía internet.

En relación al *ciberburrier* y el delito de receptación, hay un primer momento en el que el *ciberburrier* recibe dinero en su cuenta, lo cual podría ser calificado como un delito permanente, porque depende de la voluntad del agente para que el resultado lesivo permanezca en el tiempo. Pero como la doctrina y jurisprudencia han indicado, para que el agente sea calificado como autor del delito de receptación, no debió intervenir en el delito previo, sino que, por el contrario, el agente tendría que haber participado después de haberse consumado el delito anterior. Y como hemos analizado, la contribución del *ciberburrier* es imprescindible para consumar el delito de fraude informático. En vista que el *ciberburrier* es quien transfiere el dinero a la cuenta que el autor del delito de fraude informático le indicará, de esta manera

recién se tiene provecho ilícito del dinero del titular de la cuenta bancaria. Por estos motivos el *ciberburrier* no puede tener responsabilidad como autor del delito de receptación.

En este último capítulo he explicado los motivos por los cuáles el *ciberburrier* no puede ser cómplice del delito de fraude informático, básicamente porque no se pueden obtener indicios fuertes, plurales, concordantes y convergentes que demuestren que el *ciberburrier* tenía conocimiento preciso sobre el origen del dinero que recibe en su cuenta bancaria. Pero esa situación es vencible según el contexto delictivo, las reglas de la lógica o las máximas de la experiencia que deberá aplicar el Juez. Por ejemplo, puede ocurrir que el autor del delito de fraude informático no le otorga al *ciberburrier* los verdaderos detalles acerca de la procedencia del dinero, porque lo que le interesa es contar con su apoyo para poder tener el dinero en su cuenta bancaria, pero también es posible que el autor del delito de fraude informático sí dé a conocer al *ciberburrier* que el dinero que va a recibir en su cuenta bancaria proviene de un fraude informático. Este supuesto debería estar reforzado por pruebas, como por ejemplo, el vínculo familiar o amical entre los actores del delito, los antecedentes delictivos que tengan, trabajar en una misma entidad bancaria, mensajes o llamadas que demuestren este conocimiento, etc.

No obstante, al no contar, en principio, con pruebas directas que acrediten el conocimiento del *ciberburrier* de su participación como cómplice en el delito de fraude informático, considero que la responsabilidad penal del *ciberburrier* estará basada en los indicios que se puedan probar de su participación y/o autoría en un delito, estos deben ser fuertes, plurales, concordantes y convergentes, de esa manera se evitará tener contraindicios que puedan rebatir su responsabilidad. Es por ello que pienso que la responsabilidad penal del *ciberburrier*, en líneas generales, se ajusta más a la de autor en el delito de lavado de activos.

Según lo desarrollado en la tesis, el lavado de activos es un delito muy complejo, pues tiene diferentes modalidades típicas, aunque soy de la postura de que su estructura normativa denota que es un delito instrumental; es decir, sirve de medio para evitar la identificación del origen de las ganancias o bienes que se puedan obtener de un delito previo. En esta misma línea, el Acuerdo Plenario 3-2010 de la Corte Suprema del Perú, en su fundamento jurídico N°33 ha señalado lo siguiente:

> La prueba sobre el conocimiento del delito fuente y del conjunto de los elementos objetivos del lavado de activos será normalmente la prueba indiciaria -no es habitual, al respecto, la existencia de prueba directa-. La prueba indiciaria es idónea y útil para suplir las carencias de la prueba directa.

Considero que la actuación del *ciberburrier*, al apoyar o facilitar un delito (fraude informático), encaja de mejor manera en la imputación de autoría de lavado de activos. Quiero apoyar mi postura en primer lugar, en el artículo 26° del Código Penal Peruano, el cual dice que:

> Las circunstancias y cualidades que afecten la responsabilidad de algunos de los autores y partícipes no modifican las de los otros autores o partícipes del mismo hecho punible.

En segundo lugar, el artículo 10° del DL N°1106, Decreto Legislativo de lucha eficaz contra el lavado de activos y otros delitos relacionados a la minería ilegal y crimen organizado, en su segundo párrafo, señala que: "El origen ilícito que conoce o debía presumir el agente del delito podrá inferirse de los indicios concurrentes en cada caso".

Además, ha de considerarse el Acuerdo Plenario N°3-2010 en su fundamento jurídico N° 34:

> Empero, a partir de los aportes criminológicos, la experiencia criminalística y la evolución de la doctrina jurisprudencial, es del caso catalogar algunas aplicaciones de la prueba indiciaria, sobre la base cierta de la efectiva determinación de actos que sean susceptibles de ser calificados como irregulares o atípicos desde una perspectiva financiera y comercial y que no vienen sino a indicar en el fondo la clara intención de ocultar o encubrir los objetos materiales del delito.
>
> Que además señala lo siguiente:
>
> B. Se han de examinar aquellos indicios relativos al manejo de cantidades de dinero que por su elevada cantidad, dinámica de las transmisiones, utilización de testaferros, depósitos o apertura de cuentas en países distintos del de residencia de su titular, o por tratarse de efectivo pongan de manifiesto operaciones extrañas a las prácticas comerciales ordinarias.

En ese sentido, pienso que son ejemplos de indicios fuertes, convergentes y plurales: brindar su número de cuenta bancaria, las diversas transferencias bancarias que ejecuta el *ciberburrier*, y el pago de importantes comisiones por recibir y reenviar dinero. Asimismo, la doctrina y jurisprudencia también han señalado que los indicios pueden ser los móviles que motivan al agente a cometer un delito. En el presente caso, pienso que se trata del móvil de lucro, ya que al *ciberburrier* se le pagará una comisión por esta intermediación. Estos indicios me parecen fuertes, pues una persona prudente no brindaría su número de cuenta del banco

fácilmente para recibir dinero de otra persona que lo contacta y después reenviarlo a cambio de un pago por esta intermediación. Es de inferirse que este comportamiento del *ciberburrier* es doloso, puesto que conoce o presume que está inmerso en un proyecto delictivo. Lo que será difícil demostrar es que tenía conocimiento exacto del origen preciso del dinero. Por ello es que postulo que su conducta se adecua más al de ser autor en el delito de lavado de activos.

Dado que el Decreto Legislativo N° 1106 contiene una cláusula general en su artículo 10°, la cual estipula que los activos que se pretenden lavar pueden tener la procedencia de cualquier actividad criminal, pienso que al *ciberburrier* se le puede imputar la autoría en el delito de lavado de activos, porque se le puede atribuir la representación del alto riesgo delictivo que implica brindar su número de cuenta bancaria para recibir un dinero y luego reenviarlo a cambio de una comisión.

Finalmente, el delito de lavado de activos es un delito pluriofensivo y doloso que, dependiendo de sus modalidades, admite el dolo eventual, pues para su imputación se requiere que el sujeto conozca que los bienes o dinero provienen de una actividad criminal, o que al agente se le pueda atribuir la representación del alto riesgo de la procedencia delictiva, siendo el último aspecto que encuadra con el comportamiento del *ciberburrier*.

Conclusiones

En la actualidad, somos conscientes del gran desarrollo e influencia de las tecnologías de la información y la comunicación (TIC). Por ello podemos observar que gran parte de la criminalidad se realiza en el ciberespacio, el cual es un entorno virtual donde se rompen las barreras de tiempo y espacio, pues los delitos informáticos pueden ser cometidos desde cualquier parte del mundo con acceso a internet, y además pueden cometerse delitos de forma masiva, haciendo uso de la tecnología.

Los delitos informáticos no pueden ser vistos sólo como un tipo de delincuencia perpetrada a través de medios informáticos, ya que con los delitos informáticos se sobredimensionan los ataques a bienes jurídicos clásicos, lo cual exige nuevas necesidades de protección.

El delito de fraude informático es un delito de resultado porque requiere para su consumación el perjuicio de un tercero.

La intervención del *ciberburrier*, al recibir y reenviar dinero a través de internet sirve para facilitar la consumación del delito de fraude informático.

Todo comportamiento de una persona tiene un sentido social; por lo tanto, el dolo del agente no se puede describir, sino se imputa a partir de las circunstancias que aportan para determinar si socialmente se aprecia como un actuar doloso. Para esto se debe recurrir a las reglas de la experiencia que tengan un amplio consenso social. Y son estas máximas de la experiencia las que permiten valorar a un Juez que cualquier ciudadano que acepta recibir un dinero en su cuenta bancaria para luego reenviarlo a otra cuenta a cambio de una importante comisión, puede representarse el peligro de estar involucrado en una actividad delictiva.

Referencias

Aguirre Salas, Hipólito. "Criminalística y cadena de custodia". *Revista de Derecho Penal y el Derecho Procesal*. (2014).

Arbulú Martínez, Víctor. *Temas de derecho informático: Delitos informáticos, contratación electrónica, protección jurídica de programas informáticos*. Perú: CEPREDIM, Centro de Producción Editorial e Imprenta.- UNMSM, 2002.

Arigaby Molina, José. *Derecho penal: Parte General*. Buenos Aires: Ediar,1972.

Bajo Fernández, Miguel. *Manual de derecho penal: Parte especial*. Madrid: Ceura, 1990.

Barros, Oscar. *Tecnologías de la información y su uso en gestión*. Chile: McGraw Hill, 1998.

Betham Jeremias, E. Gomez de Castro, José. *Tratado de las pruebas judiciales sacado de los manuscritos*. Madrid: T. Jordan, 1835.

Blossiers, Juan, Calderon, Sylvia. *Delitos Informáticos(En la Banca)*. Lima: Rao, 2000.)

Bramont – Arias, Luis. "Teoría General del Delito: El tipo penal*." Derecho y sociedad* (1996): 188-194.

Bramont – Arias, Luis "Delitos informáticos", *Revista Peruana de Derecho de la Empresa, Derecho informático Y Teleinformática Jurídica,* núm. 51 (2000)*:* 82-93.

Burgos, Mata Álvaro. "El Delito Informático," Acta *Académica.* Núm. 47 (2010): 175-198.

Cabral, Cristian Javier. *Delito de lavado de dinero. Antecedentes internacionales, relación con el terrorismo y medio de desarrollo, Delitos Económicos*. Argentina: Editorial Ministerio de Justicia y Derechos Humanos de la Nación, 2013.

Cabrera Freyre, Raúl Peña. *Delitos contra el Patrimonio – estudios de derecho penal parte especial*.3ra edición. Perú: Motivensa SRL, 2021.

Chang Kcomt, Romy "Dolo eventual e imprudencia consciente: reflexiones entorno a su delimitación." *Derecho y Sociedad* N° 36 (2011): 255-266.

Código Penal Peruano, abril de 1991.

Conapoc. *Diagnóstico Situacional Multisectorial sobre la Ciberdelincuencia en el Perú*. Minjus, (2020): 1-74.

Consulado de Europa. *Convenio Sobre la Ciberdelincuencia*. Budapest: Serie de Tratados Europeos Nº 185 , 2001.

Creus Carlos. *Derecho penal Parte especial*, 6ta edición, Tomo I. Buenos Aires: Astrea, 1998.

Delgado Martín, Joaquin. "La prueba electrónica en el proceso penal". *Diario La Ley*. Nº 8167 (2013):1-29.

Durand Valladares, Raúl. “Los delitos informáticos en el Código Penal Peruano*” Revista Peruana de Ciencias Penales*, Nº. 11(2002): 305-328

Fernández Peruelo, Javier Gustavo. *Derecho Penal e Internet*. España: Lex Nova, 2011.

Figueroa Vavarro, Carmen. "El aseguramiento de las pruebas y la cadena de custodia". *La Ley Penal*, núm. 84 (2011): 5-14.

García Cantizano, María del Carmen .*Falsedades Documentales* en el Código Penal de 1995. Valencia: Tirant lo blanch, 1997.

García Cavero, Percy. *Derecho Penal Económico*. Lima: Instituto pacifico, 2015.

García Cavero, Percy. *Derecho Penal Parte General*. 3ra Edición. Perú: Ideas Solución Editorial SAC, 2019.

Gutiérrez, Francés María. *Fraude Informático y estafa*. Madrid: Centro de Publicaciones del Ministerio de Justicia, 1991.

Hurtado Pozo, José. *Manual del Derecho Pena*l. 3ra Edición. Perú: Editora Jurídica Grijley E.I.R.L., 2005.

Jiménez Herrera, Juan Carlos. *Manual de Derecho Penal Informático.* Lima: Jurista Editores EIRL, 2017.

Lessig, Lester. *El Código y otras leyes del ciberespacio*. Madrid: Grupo Santillana, 2001.

Maier, Julio *Derecho Procesal Penal*. Tomo I. 2° edición. Buenos Aires: Editores del Puerto, 2004.

Mazuelos, Coello Julio. “Modelos de imputación en el Derecho penal informático,” *Derecho Penal y criminología*, 28, núm. 85 (2007): 37-54.

Meini Mendez, Ivan. *Lecciones de Derecho Penal, Parte General*. Lima: 2014.

Ministerio del Interior. “Manual de Evidencia Digital”. (2020): 1-64 https://cdn.www.gob.pe/uploads/document/file/1303962/DWP-ManualParaRecojo-EVIDENCIA.DIGITAL.pdf?v=1600289472

Miró Linares, Fernando. “La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen.” *Revista electrónica de la ciencia penal y criminología*, (2011): 1-55 http://criminet.ugr.es/recpc/13/recpc13-07.pdf

Miró Linares, Fernando. *Fenomenología y Criminología de la delincuencia en el ciberespacio.* Madrid: Ediciones Jurídicas y Sociales S.A.C, 2012.

Miró Linares, Fernando. "La respuesta penal al ciberfraude: Especial atención a la responsabilidad de los muleros del phishing". *Revista Electrónica de Ciencia Penal y Criminología*. (2013): 1-56 http://criminet.ugr.es/recpc/15/recpc15-12.pdf

Miró Linares, Fernando. *Crimen, Oportunidad y Vida Diaria*. Madrid: Dykinson, 2015.

Miró Linares, Fernando. "Cibercrimenes Economicos Y Patrimoniales". *Memento Práctico. Penal Económico y de la Empresa* (2016): 497-541.

Montenegro, María Luisa. "Cooperación Internacional: Tramitación, obtención de pruebas, e incorporación de pruebas y evidencias". *Revista Jurídica Ministerio Público,* N°70 (2017): 63-85.

Muñico Patilla, Shirley. "La lucha contra el lavado de activos: ¿estamos avanzando o retrocediendo? ¿realmente "nuestras autoridades están luchando contra la criminalidad"? ¿qué falta?»". *Revista.Ius.*et 1, n.º 1, (2018): 69 – 87.

Muñoz Conde, Francisco, Hassemer Winfried. *Introducción a la criminología y al Derecho Penal*. Valencia: Tirant Lo Blanch, 1989.

Muñoz Conde, Francisco. *Teoría General Del Delito*. Santa Fe de Bogotá-Colombia: Editorial Temis S. A, 1999.

Muñoz Conde Francisco. *Teoría general del Delito*. Bogotá: Themis,2004.

Naresh, Suman. *Sociedad de la Información: los nuevos pobres*. Quark: Ciencia, medicina, comunicación y cultura, Nº 17, 1999.

Nessi Martin Alan. "Manual de evidencia digital". (2017):1-64 https://www.mpfn.gob.pe/Docs/0/files/manual_evidencia_digital.pdf

Núñez Ponce, Julio. "Apuntes sobre la protección jurídica del Software o programas de computadoras". *Ius Et Praxis*, 007, (1986): 1 129- 133 https://doi.org/10.26439/iusetpraxis1986.n007.3337.

Oré Guardia, Arsenio . Loza Davalos, Giulliana. "La estructura del Proceso Común en el Nuevo Código Procesal Peruano". *Derecho y Sociedad (*2005): 163-177.

Oré Sosa, Eduardo. *Delictum, apuntes de derecho penal*. Perú : Editores del Centro, 2022.

Orts Berenguer, Enrique. Gonzáles Cussac, José Luis. *Compendio de Derecho Penal Parte General*. Valencia: Tirant lo blanch,2019.

Peña Gonzáles, Oscar. *Teoría del delito: manual práctico para su aplicación en la teoría del caso.* Perú: Asociación Peruana de Ciencias y Conciliación - APECC., 2010.

Peña Cabrera Freyre, Alonso. *Derecho penal. Parte especial,* Tomo II. Lima: Idemsa, 2013.

Ríos Arenaldi, Jaime. "El consentimiento en materia penal", *Revista Politica Criminal*, 1, núm. 1, (2006): 1-37.

Rivera Avalos, Zoraida. "Ciberdelincuencia: Pautas para una investigación fiscal especializada". Oficina de análisis estratégico contra la criminalidad (2021):1-68. https://cdn.www.gob.pe/uploads/document/file/1669400/CIBERDELINCUENCIA%2

0EN%20EL%20PERÚ%20-%20PAUTAS%20PARA%20SU%20INVESTIGACIÓN%20FISCAL%20ESPECIALIZADA%20-%2015%20FEBRERO%202021.pdf

Rodríguez Devesa, José María. *Derecho Penal español: Parte General*. Madrid: Artes Gráficas Carasa, 1981.

Rodríguez C. & Demetrio E. Curso de Derecho penal Parte General. España: Ediciones Experiencia, S.L. , 2010.

Rojas,Fidel. *Jurisprudencia Penal y Procesal Penal*. Lima: Idemsa 2000.

Roy Freyre Luis. *Manual de Derecho penal. Parte especial*. Lima: Eddili 1986.

Roxin, Claus. "Problemas de Autoría y Participación en la criminalidad organizada". *Revista Penal N°* 2, (1998): 62-92.

Sánchez Brot, Luis. *Lavado de dinero. Delito transnacional*. Buenos Aires: La Ley. 2002.

Sánchez, James Reátegui. *Manual de derecho penal. Parte especial Delitos contra la vida, contra el patrimonio y otros*. Lima: Pacífico Editores. SAC, 2015.

Sánchez Hernández, José Luis. "WhatsApp, prueba válida en juicio". *Revista del Ilustre Colegio de Abogados de Salamanca*, nº. 12, (2016): 1-71.

Sanz Morán, Ángel José. *El concurso de delitos en la reforma penal*. Madrid: Consejo General del Poder Judicial, 1995.

Silva Sánchez, Jesús María. *Aproximación al Derecho Penal Contemporáneo*. Barcelona: Bosch, 1992.

Talavera Elguera, Pablo. *La Prueba en el Nuevo Proceso Pena: Manual del derecho probatorio y de la Valorización de las Pruebas en el Proceso Penal Común*. Lima: Academia de la Magistratura, 2009.

Terragni, Marco Antonio. *El Delito Culposo.* Chile: Editorial Rubinzal –Culzoni, 1984.

Tirado Estrada, Jesús. "Cooperación Judicial internacional en el ámbito iberoamericano. Balance y Perspectivas. Especial referencia a los procesos de instauración de medidas estructurales de relación, organización y coordinación." *Mecanismos de Cooperación Judicial Internacional* (2014): 143-191.

Urbano Castrillo, Eduardo. *Delincuencia Informática. Tiempos de cautela y amparo*. Pamplona: Thomson Reuters, Aranzadi, 2012.

Varela Casimiro, A. *Valoración de la prueba.* Buenos Aires: Astrea,1999.

Vasquez Rossi, Jorge. *Derecho Procesal Penal*. Tomo I. Argentina: Editorial Rubinzal – Culzoni, 1995.

Villavicencio Terreros, Felipe. *Derecho Penal: Parte general.* Perú, Grijley, 2013.

Villavicencio Terreros, Felipe. *Derecho penal básico*. Lima: Pontificia Universidad Catolica del Peru, 2019.

Vives Antón, Tomas Salvador. *Derecho Penal. Parte Especial*. Valencia: Tirant lo blanch, 1993.

Vizcardo, Hugo y Silfredo, Jorge. "Tipificación De Los Delitos Informáticos Patrimoniales En La Nueva Ley De Delitos Informáticos N°30096." *Alma Mater* 1, núm.1 (2014):69-80.