La relación concursal entre los tipos de fraude informático en el ordenamiento jurídico chileno

Profesor Guía: José Luis Guzmán Dalbora

Estudiante: Enrique Antonio De la Fuente Vásquez

Índice

Introducción página……. 3

1. **Fraude informático: Panorama en la doctrina y el Derecho comparado…..... 4**
    1. **Estos delitos en la legislación extranjera. …….. 4**
    2. **El Convenio N° 185, del Consejo de Europa, sobre la Ciberdelincuencia (Convenio de Budapest).....6**
    3. **La introducción del Convenio de Budapest al ordenamiento jurídico chileno…….9**
    4. **Conclusiones preliminares……..13**
2. **Fraude informático en la legislación chilena**
    1. **El fraude informático de la ley 21.453: actividad típica, objeto material, elementos subjetivos de lo injusto. ……15**
    2. **2° El fraude informático del Código penal: actividad típica, objeto material, elementos subjetivos de lo injusto. …… 21**
    3. **Bien jurídico protegido en el fraude informático. …….. 26**
    4. **Conclusiones preliminares. ……32**
3. **Relaciones concursales del fraude informático de la Ley 21.459 y el del artículo 468 del Código penal. …… 35**
    1. **Vigencia simultánea de estas defraudaciones o derogación tácita de la precedente en el tiempo. …….35**
    2. **Problemas concursales del fraude informático y determinación del concurso aparente de leyes o concurso de delitos ……37**
    3. **El concurso aparente de leyes entre el fraude informático de la Ley 21.459 y el del artículo 468 del Código penal…… 40**
    4. **Conclusiones preliminares …… 46**

Conclusiones finales…….. 48

Bibliografía …… 50

Introducción

El acelerado desarrollo tecnológico y la creciente digitalización de las actividades humanas han transformado de manera profunda la forma en que interactuamos, producimos y nos relacionamos. Este fenómeno ha dado lugar a nuevas modalidades delictivas que desafían los marcos normativos tradicionales, obligando al Derecho penal a adaptarse para enfrentar conductas que lesionan bienes jurídicos mediante medios informáticos. Entre estas figuras, el fraude informático se posiciona como uno de los delitos más relevantes, tanto por su frecuencia como por la complejidad dogmática que plantea.

El problema central de esta investigación surge porque, en el ordenamiento jurídico chileno, actualmente coexisten dos tipos penales de fraude informático, incorporados con escasa diferencia temporal. El primero fue introducido el 20 de junio de 2022 mediante la Ley N.º 21.459, mientras que el segundo se incorporó al Código Penal el 17 de agosto de 2023, a través de la Ley N.º 21.595. Esta situación plantea interrogantes sobre su naturaleza jurídica, su ubicación sistemática y los desafíos que genera para la coherencia del sistema penal. Por ello, el objetivo de este trabajo es aportar claridad sobre estas cuestiones y ofrecer conclusiones que orienten una correcta aplicación de ambos tipos.

Para cumplir dicho propósito, el primer capítulo examinará la regulación del fraude informático en el derecho comparado y el proceso de incorporación del Convenio N.º 185 del Consejo de Europa (Convenio de Budapest) al ordenamiento jurídico chileno.

El segundo capítulo abordará el estudio dogmático del tipo penal contenido en la Ley N.º 21.459, analizando su actividad típica, objeto material, elementos subjetivos y problemas concursales. Asimismo, se estudiará el nuevo tipo de fraude informático del artículo 468 del Código Penal, destacando sus diferencias y similitudes con la regulación anterior, y se determinará el bien jurídico protegido, discutiendo si esta figura debe entenderse como una defraudación patrimonial, un delito informático o una figura pluriofensiva.

Finalmente, el tercer capítulo se centrará en la relación concursal entre ambos tipos, resolviendo si existe derogación tácita, concurso aparente de leyes o concurso de delitos.

Fraude informático: Panorama en la doctrina y el Derecho comparado

1.Estos delitos en la legislación extranjera.

La evolución de la tecnología en el último siglo ha sido explosiva. Desde el inicio del siglo XX el desarrollo de la ingeniería y la maquinaria a favor de la producción en masa con la revolución industrial provocaron grandes cambios en nuestra sociedad. En esa época, la transformación de las condiciones de vida y dinámicas sociales provocaron nuevas formas de delincuencia, que obligaron al Derecho penal a mutar para adaptarse a las nuevas necesidades. Más de medio siglo después, desde los años 60, con el progreso de las computadoras y la informática, se ha producido un fenómeno similar.

Se ha especulado que son varios los aspectos de la tecnología informática que fomentan la aparición de nuevas modalidades delictivas. La realidad es que la interconexión digital, el anonimato que existe en el ciberespacio, la incorruptibilidad material de los datos almacenados en sistemas informáticos, lo manipulable de la información digital y la desterritorialización de las actividades en este tipo de delitos[1], provocan una doble relevancia de los sistemas de procesamiento, tratamiento y comunicación electrónica. Estos sistemas informáticos son relevantes, en primer lugar, como posible objeto de conductas ilícitas (soporte físico del sistema informático) y, en segundo como instrumento que facilita, asegura o agrava los efectos de ilícitos tradicionales[2]. Dentro de la delincuencia informática, se distingue un sector de ella que es especialmente relevante, la llamada *"ciberdelincuencia económica",* dado que este tipo de ciberdelincuencia se corresponde con el 85% de los delitos informáticos cometidos[3].

Lo anterior ha provocado que una gran cantidad de Estados modernizaran sus legislaciones, para que estas sean capaces de hacer frente a estas nuevas modalidades de delincuencia. Esto es especialmente importante respecto a la ya mencionada *"ciberdelincuencia económica",* dado que los tipos patrimoniales tradicionales no son capaces de captar las conductas lesivas contra el patrimonio que se realizan a través de sistemas informáticos. Por lo tanto, son muchos los Estados que se han visto obligados a tipificar el fraude informático.

Por ejemplo, España contempla el fraude informático en el artículo 249 del Código penal, el cual prescribe que:

---

[1] Wall D, "The Internet as a conduit for criminal activity", en April P (ed.), *Information Technology and the Criminal Justice System*, (Thousand Oaks, Sage), 2005, p. 77.
[2] GUTIERREZ, *Fraude informático y estafa*, Editorial Ministerio de Justicia, Madrid, 1991, p. 7.
[3] Velasco E, *"Delitos tecnológicos: definición, investigación y prueba en el proceso penal",* Editorial Sepin, Madrid, 2016, págs. 175-178.

"también se consideran reos de estafa y serán castigados con la pena de prisión de seis meses a tres años:

a) Los que, con ánimo de lucro, obstaculizando o interfiriendo indebidamente en el funcionamiento de un sistema de información o introduciendo, alterando, borrando, transmitiendo o suprimiendo indebidamente datos informáticos o valiéndose de cualquier otra manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro".

Aquí es claro que el legislador español quería mantener la relación existente entre fraude informático y estafa. Sin embargo, tal como explicaremos más adelante, en realidad estos delitos castigan dos conductas perfectamente diferenciables, y están únicamente relacionados debido a que ambos son delitos que afectan intereses patrimoniales[4].

Otro ejemplo interesante es el caso alemán. En este país, con la segunda Ley contra la criminalidad Económica de 15 de mayo de 1986, se incorporó un §263 Código penal (StGB), cuyo primer apartado reza:

"El que, con el propósito de obtener para sí o para un tercero un beneficio patrimonial ilícito, perjudique el patrimonio de otro influyendo en el resultado de un proceso de tratamiento de datos mediante la incorrecta configuración del programa, la utilización de datos incorrectos o incompletos, la utilización no autorizada de datos o cualquier otra intervención no autorizada en el proceso, será castigado con pena privativa de libertad de hasta cinco años o con multa".[5]

Aquí se puede observar que, a diferencia del caso español, no se hace referencia expresa al delito de estafa. Esto se debe a que el Congreso alemán, al momento discutir el proyecto de ley llegó a la conclusión de que es inútil intentar subsumir el tipo de fraude informático en el de estafa, dado que, salvo el perjuicio patrimonial, la concurrencia del resto de elementos de la estafa en el fraude informático es sumamente dudosa[6].

Ahora bien, en nuestro continente es interesante mirar la regulación que los Estados de Perú y Argentina han dado a este delito.

---

[4] Mayer-Calderón, "El delito de fraude informático: Concepto y delimitación", *Revista chilena de Derecho y tecnología*, VOL. 9 N°. 1, 2020, pág. 156.

[5] Traducción obtenida de Hernández, "La esperada consagración de un genuino delito de fraude informático en el Derecho penal chileno (Art 7° de la Ley N° 21.459)" en Scheechler (edit) Riveros (coord.) *Los delitos informáticos: Aspectos político-criminales, penales y procesales en la ley n° 21.459*, DER EDICIONES, Santiago de Chile, 2024, pág. 211.

[6] Ibidem, pág. 210.

En esta línea, Perú dictó su Ley 30-096, la cual tenía por objetivo adaptar la legislación d a lo exigido por el Convenio N° 185, del Consejo de Europa, del año 2001, sobre la Ciberdelincuencia[7]. Este cuerpo normativo, en su artículo 8 prescribe que:

"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".

Como observaremos más adelante, este artículo tiene una estructura muy similar a la propuesta por el Convenio de Budapest. Este tipo sigue los parámetros fijados por esta convención, y regula la conducta sancionada alrededor *de la "manipulación de sistemas o datos informáticos".*

Por otro lado, la regulación que establece el ordenamiento jurídico argentino dista un poco de las anteriormente revisadas. En este país la Ley 23.388 introdujo el fraude informático al Código penal, añadiendo el artículo 173, el cual reza así:

""El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos".

Se hace evidente que la descripción típica del fraude informático es mucho menos exhaustiva que en los casos anteriormente revisados. Aquí, a diferencia de los otros casos, no se realiza referencia alguna a los medios de ejecución. En los otros ejemplos estudiados, los tipos establecen que el fraude informático se debe cometer mediante la *"introducción, alteración, borrado, supresión, clonación de datos informáticos".* Mientras que, en el caso argentino, el legislador simplemente establece que este tipo de fraude se debe realizar mediante una *"manipulación informática",* una cláusula mucho más general, y que poco dice sobre las conductas penadas, dejando solo en claro que esta conducta al menos debe afectar al software de un sistema informático.

2. El Convenio N° 185, del Consejo de Europa, sobre la Ciberdelincuencia (Convenio de Budapest)

El Convenio de Budapest es un tratado internacional que ofrece una guía a los países para desarrollar una legislación integral contra los ciberdelitos. Actualmente, ha sido

[7] En adelante Convenio de Budapest.

ratificada por 81 países[8], entre ellos Chile, y *se considera la norma internacional más completa hasta la fecha, ya que proporciona un marco integral y coherente en contra del ciberdelito y la evidencia electrónica."*[9].

Los Estados que participaron en la negociación del Convenio fueron los miembros del Consejo de Europa, Estados Unidos, Canadá, Japón y Sudáfrica y fue suscrito el 23 de noviembre de 2001. Además, de acuerdo con lo estipulado por el artículo 37 de este cuerpo normativo, cualquier Estado que no sea parte del Consejo de Europa puede convertirse en parte mediante adhesión. Según los artículos 37 y siguientes del Convenio, la adhesión implica:

"1. Una vez que esté disponible un proyecto de ley que indique que un Estado ya ha implementado o es posible que pueda implementar las disposiciones del Convenio de Budapest en su legislación nacional, el ministro de Relaciones Exteriores (u otro representante autorizado) deberá enviar una carta dirigida al secretario general del Consejo de Europa en la que manifieste el interés de su Estado en adherirse al Convenio de Budapest.

2. Una vez que exista consenso entre los actuales Estados Parte del Convenio, se invitará al Estado a adherirse.

3. Las autoridades de ese Estado deberán formalizar sus procedimientos internos similares a la ratificación de cualquier tratado internacional antes de depositar el instrumento de adhesión ante el Consejo de Europa"[10].

Al respecto de su estructura, este tratado cuenta con un total de cuatro capítulos, los cuales versan sobre: terminología, medidas que deberán adoptarse a nivel nacional, cooperación Internacional y disposiciones finales. Los capítulos que interesan, para los efectos de este trabajo, son los dos primeros.

En el primer capítulo, específicamente el artículo primero, se entrega distintas definiciones. Específicamente, se define qué son los "*datos informáticos", "sistemas informáticos", "proveedor de servicios" y "datos relativos al tráfico".* Estas definiciones, salvo la última serán posteriormente recogidas en el artículo 15 de la Ley 21.459[11], y definirán estos elementos de la siguiente manera:

a) Por "sistema informático" se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno

[8] https://www.coe.int/en/web/cybercrime/the-budapest-convention.
[9] Consejo de Europa Estrasburgo, Francia División de Ciberdelito. DG, *"Adhesión al Convenio de Budapest sobre la Ciberdelincuencia: Beneficios",* 2022, pág. 1.
[10] Ibidem.
[11] En Adelante LDI.

de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.

b) Por "datos informáticos" se entenderá toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función;

c) Por "proveedor de servicios" se entenderá:

i. toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático, y

ii. cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios de este;

El segundo capítulo del Convenio se titula "Medidas que deberán adoptarse a nivel nacional" y se divide en tres secciones: Derecho penal sustantivo, Derecho procesal y jurisdicción.

La sección que nos interesa es la primera, la relativa al Derecho penal sustantivo. Esta cuenta con 5 títulos:

1. Delitos contra la confidencialidad, la integridad y la disponibilidad de datos y sistemas informáticos: en este título encontramos los delitos de acceso ilícito, interceptación ilícita, ataques contra la integridad de los datos, ataques contra la integridad del sistema, abuso de los dispositivos.[12]
2. Delitos informáticos: es el título que nos resulta relevante, ya que además de la falsificación informática, también se encuentra regulado **el fraude informático**[13].
3. Delitos relacionados con el contenido: en esta sección lo que encuentra regulación son los delitos relacionados a la pornografía infantil[14].
4. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines: tal como dice el título, aquí se encuentran regulados los delitos relativos a la infracción de la propiedad intelectual y de los derechos afines.
5. Otras formas de responsabilidad y de sanción: aquí se encuentra la regulación relativa a la tentativa y complicidad, responsabilidad de las personas jurídicas y sanciones y medidas.

Tal como mencionamos anteriormente, el título que nos interesa es el segundo, ya que aquí está regulado el fraude informático. En su artículo 8, el convenio prescribe los siguientes lineamientos para la tipificación para el delito de fraude informático:

"Artículo 8 - Fraude informático

[12] Están en los artículos 2 al 6 respectivamente.
[13] En los artículos 7 y 8 respectivamente.
[14] Artículo 9 del Convenio de Budapest.

Las Partes adoptarán las medidas legislativas o de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante:

a. la introducción, alteración, borrado o supresión de datos informáticos;

b. cualquier interferencia en el funcionamiento de un sistema informático, con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona".

3. La introducción del Convenio de Budapest al ordenamiento jurídico chileno

3.1 El proceso de ratificación del Convenio de Budapest.

El Estado chileno depositó el instrumento de adhesión a este instrumento el día 20 de abril de 2017. Este mismo entró en vigor el 28 de agosto de 2017, con la publicación oficial del decreto de promulgación, contenido en el Decreto N°83 del Ministerio de Relaciones Exteriores.

En esta promulgación, Chile hizo cuatro reservas. La primera de ellas es relativa al artículo 4 N°2[15] de la convención de Budapest. Este artículo se refiere al ataque a la integridad de los datos. Esta reserva se hizo debido a los "daños graves". En esencia, *"esta limitación está dada por la elasticidad o del concepto "grave" ante ataques a la integridad de los datos, lo que amenaza el principio de taxatividad del derecho penal"*[16].

La segunda reserva se hizo respecto al artículo 6 del Convenio, en cuanto al abuso de dispositivos. Específicamente, la reserva se hace en los términos de que el Estado chileno no tipificará el abuso de dispositivos "*en la medida que ello no afecte la venta, distribución o cualesquiera otras formas de puesta a disposición de los elementos mencionados en el inciso 1 a) ii) del citado Artículo.".*[17]

La tercera reserva no es relativa a las normas relativas a las normas pertenecientes al primer título del capítulo II – Derecho penal sustantivo-, sino respecto al título III, es decir, el de jurisdicción, específicamente el artículo 22 N°1 letra d. Chile no tendrá jurisdicción cuando alguno de los ilícitos establecidos en esta convención sea realizado "*por uno de sus*

[15] Artículo 4 - Ataques a la integridad de los datos.
1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos.
2. Las Partes podrán reservarse el derecho a exigir que los actos definidos en el párrafo 1 comporten daños graves.

[16] Becker Viollier, "La implementación del Convenio de Budapest en Chile: Un análisis a propósito del proyecto legislativo que modifica la Ley 19.223", *Revista de Derecho Universidad de Concepción,* N°248, 2020, pág. 79.

[17] DS ([Relaciones Exteriores] N° 83/2017), de 28 de agosto de 2017.

nacionales, si el delito es susceptible de sanción penal en el lugar en el que se cometió o si ningún Estado tiene competencia territorial respecto del mismo"[18] .

Finalmente, la última reserva que realiza el Estado chileno es relativa al apartado de cooperación internacional. Específicamente, la reserva es relativa al artículo 29 párrafo 4 de este instrumento, es decir, que se podrá "*denegar la solicitud de asistencia internacional en caso de que la conducta perseguida no esté tipificada en Chile al momento del requerimiento"*[19]. Se trata, evidentemente, del principio de doble incriminación.

3.2 La evolución del fraude informático en la tramitación de la Ley 21.459

Otro aspecto que es interesante analizar, son las adecuaciones normativas que se contienen en el boletín N°12.192-25[20], que busca modificar la Ley 19.223, específicamente respecto del tipo de fraude informático.

En su redacción original, el tipo de fraude informático se encontraba en el artículo 6 de aquella ley. Este artículo disponía lo siguiente:

"Artículo 6°.- Fraude informático. El que, causando perjuicio a otro y con la finalidad de obtener un beneficio económico ilícito para sí o para un tercero, utilice la información contenida en un sistema informático o se aproveche de la alteración, daño o supresión de documentos electrónicos o de datos transmitidos o contenidos en un sistema informático"

Como podemos observar, este articulado presenta una regulación bastante diversa a lo exigido por el artículo 8 del Convenio y también a lo estipulado en el artículo 7 de la LDI. En primer lugar, ninguna de las normas anteriormente mencionadas hace referencia a la "utilización de la información contenida en un sistema informático". En segundo lugar, este artículo no hace ninguna referencia al verbo rector que se usa en el tipo de fraude contenido en la LDI, es decir, la *"manipulación"*. Finalmente, este no contempla la segunda modalidad del artículo 8 de la Convención, es decir, no tipifica la hipótesis de que alguien cause perjuicio patrimonial *"mediante cualquier interferencia al sistema informático"*. Por esto mismo, en los posteriores cambios que se hicieron a esta redacción, se agregaron los conceptos de *"manipulación",* además de penar cualquier interferencia al sistema informático, dejando como resultado el artículo 7 de la LDI que prescribe lo siguiente:

"Artículo 7°. - Fraude informático. El que, causando perjuicio a otro y con la finalidad de obtener un beneficio económico para sí o para un tercero, manipule un sistema informático, mediante la introducción, alteración, daño o supresión de datos informáticos o a través de cualquier interferencia en el funcionamiento de un sistema informático, será penado".

[18] Artículo 22 N° 1 letra d, del Convenio de Budapest.
[19] DS ([Relaciones Exteriores] N° 83/2017), de 28 de agosto de 2017.
[20] Que terminaría convirtiéndose en la LDI.

3.3 Publicación de la Ley 21.459 y la derogación de la Ley 19.223

La primera Ley que reguló conductas referentes a los delitos informáticos fue la N.º 19.223, dictada el 7 de junio de 1993. Esta optó por una regulación independiente de estas figuras, fuera del Código penal y estaba orientada a proteger un nuevo bien jurídico que ha surgido con el uso de las modernas tecnologías computacionales.

Se estructuraba sobre la base de cuatro artículos, destinados exclusivamente a regular comportamientos delictivos que se vinculan con el sabotaje informático (artículos 1º y 3º) y con el espionaje (artículos 2º y 4º). Con las conductas tipificadas en esta Ley, no era posible castigar las que suponen un fraude informático, el cual se entiende como "la derogación de perjuicio y desplazamiento patrimonial a través de sistemas informáticos"[21].

Debido a que la regulación ofrecida por la Ley 19.223 quedó obsoleta con los nuevos avances tecnológicos y la evolución de la cibercriminalidad, Chile se vio en la necesidad de actualizar su legislación en esta materia. Es por esto por lo que, el 28 de agosto de 2017 se publicó el Decreto N.º 83 del Ministerio de Relaciones Exteriores, que promulgó el Convenio de Budapest. El 20 de junio de 2022 se publica la LDI, que actualiza la legislación chilena en materia de delitos informáticos, adecuándose a las exigencias del Convenio de Budapest.

Existen tres grandes diferencias entre estas leyes[22]:

1° La cantidad de delitos regulados. La ley 19.223 regula conductas relativas al espionaje y sabotaje informáticos. La LDI regula conductas mucho más variadas.

2° Relacionado con lo anterior, la Ley 19.223 solo regula conductas relacionadas con el espionaje y el sabotaje informáticos. Por otro lado, LDI regula conductas relacionadas al sabotaje informático, espionaje informático, falsificación informática, receptación de datos informáticos, fraude informático y abuso de los dispositivos. **Por lo tanto, se tipifica por primera vez el fraude informático en el ordenamiento jurídico chileno.**

3° La tercera diferencia entre la Ley Nº 19.223 y la LDI radica en que la primera se limita a regular delitos, abarcando la segunda, en cambio, tipos penales, circunstancias modificatorias de la responsabilidad penal e incluso de reglas que atañen al proceso penal que se siga para la persecución de un delito informático.

Como se ha mencionado anteriormente, la dictación de la LDI fue fundamental para modernizar el aparato punitivo chileno, en lo relativo a la persecución de los delitos informáticos. Esto tiene importancia por dos motivos. El primero se relaciona con el gran

[21] Mayer-Vera, "La nueva Ley de delitos informáticos", *Revista de Ciencias Penales*, sexta época, vol. XLVIII, N.º 3, 2022, p. 152.
[22] Ibidem.

aumento de la ciberdelincuencia en nuestro país. Solo para dar un ejemplo, entre 2016 y 2017 hubo un aumento de un 74% de este tipo de delincuencia[23]. El segundo es relativo al limitado catálogo de delitos informáticos que ofrecía la Ley 19. 223, lo que provocaba que muchas conductas que hoy son consideradas parte de esta clase de delitos quedarán en la impunidad.

Esto último se hacía aún más evidente al hablar del fraude informático. Si bien esto se profundizará en los próximos capítulos, es importante mencionar que las conductas que constituyen el fraude informático son difíciles, o mejor dicho imposibles de captar por los tipos penales tradicionales y los presentes en la Ley 19.223, al menos de manera directa. Esto se puede representar bien con dos ejemplos, que demuestran que, sin un tipo de fraude informático en los términos de la Ley 21.459, estos actos quedarían en la impunidad. Estos ejemplos son la relación del fraude informático con la estafa y que los tipos presentes en la Ley 19.223 sólo pueden castigar fraudes informáticos de manera indirecta.

El vínculo entre fraude informático y estafa es bastante claro. Sin embargo, la estructura típica del fraude informático es distinta de la estafa, lo que se constata en los requisitos típicos de uno y otro. En el caso de la estafa se exige un engaño que provoque un error, el que motive un acto de disposición patrimonial que provoque un perjuicio económico. Todo esto, vinculado por una relación de causalidad. El error es un fenómeno psicológico, por lo que las máquinas no pueden incurrir en el error[24]. Por dicho motivo, no puede castigarse a título de estafa la realización de conductas fraudulentas respecto de o contra un sistema de tratamiento automatizado de la información. Estas últimas conductas se relacionan con fraudes informáticos y no pueden ser castigadas sin un tipo especial.

Como se dejará en claro más adelante, el fraude informático se vincula con la generación de un perjuicio patrimonial, mediante la manipulación de datos o sistemas informáticos[25]. El problema es que ninguno de los tipos de la Ley 19.223 hacía referencia a la provocación de un perjuicio por alguno de estos medios, lo que provocó que la jurisprudencia haya tenido que castigar indirectamente estas conductas. En esta línea, si bien con la Ley 19.223 no se podía castigar el hecho de causar un perjuicio con la manipulación de los datos informáticos, si se podía castigar el hecho de acceder ilícitamente al sistema, con el tipo del artículo 2[26] de esta Ley o aplicando la sanción correspondiente al destruir estos datos[27], cuando el perjuicio se provocaba por esta vía. Sin embargo, esto resultaba problemático, ya que las sanciones a estas conductas eran bastante

[23] BOLETÍN N° 12.192-25, "INFORME DE LA COMISIÓN DE SEGURIDAD PÚBLICA.", 2019, pág. 7.
[24] Politoff-Matus-Ramírez, *Lecciones de derecho penal chileno: Parte especial*, Editorial Jurídica de Chile, Santiago, 2005, p. 412.
[25] Mayer-Calderón, "El delito de fraude informático: Concepto y delimitación", *Revista chilena de Derecho y tecnología*, VOL. 9 N°. 1, 2020, p. 170.
[26] Me refiero al tipo de acceso ilícito.
[27] Aplicando el tipo de sabotaje informático, presente en el artículo 1 de la Ley 19.223.

bajas y no alcanzaban a reflejar adecuadamente el desvalor de estas conductas, resultando así insuficientes para sancionar este tipo de delito.

4° Conclusiones preliminares

De lo anteriormente revisado, podemos concluir que la mayoría de los países que introdujeron el fraude informático en sus ordenamientos jurídicos han seguido una fórmula similar.

En efecto, los tipos presentes en los ordenamientos jurídicos de España, Alemania, Perú y Chile hacen referencia a la provocación de perjuicios patrimoniales, a través de la manipulación de datos informáticos o del sistema informático. Sin embargo, el tipo español sería el único que establece que esa manipulación debe estar dirigida a provocar un perjuicio económico a través de una transferencia no consentida de activos patrimoniales, limitando de manera más precisa la conducta[28]. El caso argentino es más especial, ya que el legislador no hace una descripción tan exhaustiva de la conducta constitutiva de fraude informático, y se limita a señalar que este último constituye una *"defraudación"* a través de cualquier clase de manipulación informática o alteración de un país informático.

En segundo lugar, queda en evidencia de que el Convenio N° 185, del Consejo de Europa, sobre la Ciberdelincuencia es el modelo que la mayoría de los países utiliza para diseñar su regulación relativa a los delitos informáticos. Este cuerpo no se limita a proponer una tipificación para los delitos informáticos más comunes, sino que además propone una regulación para los delitos relativos a la difusión pornografía infantil y la afectación de la propiedad intelectual. Por su puesto, además de pronunciarse sobre el Derecho penal sustantivo, también propone una regulación bastante exhaustiva en materia de Derecho procesal y jurisdicción.

En tercer lugar, podemos concluir que la introducción del Convenio de Budapest al ordenamiento jurídico chileno se debe a una necesidad de actualizar nuestra legislación, en la materia de delitos informáticos. La regulación ofrecida por la Ley 19.223 era insuficiente para hacer frente a las nuevas formas de ciberdelincuencia. Esto debe principalmente al limitado catálogo de tipos presentes en dicha ley, sumado a la incapacidad de los tipos penales tradicionales para captar las conductas que hoy en día son sancionadas como delitos informáticos. Lo anterior provocaba que solo se pudiera castigar los actos preparatorios de fraude informático o bien que estas conductas no recibieran ningún castigo, por ser atípicas.

Es por esto por lo que la publicación de la LDI es extremadamente importante. Viene a aportar un catálogo más completo de delitos informáticos, con una redacción más

[28] Por ejemplo, en España, a diferencia de los otros países, el hecho de alterar el monto de una deuda a través de una manipulación de datos informáticos no es una conducta que se pueda sancionar a título de fraude informático.

precisa y adecuada para su nivel de desarrollo actual. Entre los delitos incorporados por la presente Ley, se encuentra el fraude informático, cuya introducción es especialmente fundamental, dado que este es uno de los ciberdelitos más cometidos y que antes de la publicación de la LDI no podía ser sancionado de manera directa. La regulación de este delito es bastante similar a la propuesta por el Convenio de Budapest, consistiendo en la provocación de un perjuicio patrimonial mediante la manipulación de datos o sistemas informáticos y que será estudiada con profundidad en el próximo capítulo.

Fraude informático en la legislación chilena

1° El fraude informático de la ley 21.453: actividad típica, objeto material, elementos subjetivos de lo injusto.

Tal como se dejó en claro en el capítulo anterior, la tipificación del fraude informático de LDI se inspira completamente en la propuesta planteada por el Convenio de Budapest. Específicamente, este instrumento establece como obligación la tipificación de la generación de perjuicio patrimonial, ya sea a través de la introducción, alteración, borrado o supresión de datos informáticos o de cualquier interferencia en el funcionamiento de un sistema informático. En ambas hipótesis se debe realizar con la intención ilegítima, dolosa o delictiva de obtener un beneficio económico para sí mismo o un tercero.

Es por esto por lo que el artículo 7 de la LDI ha terminado tipificando:

"Artículo 7°.- Fraude informático. El que, causando perjuicio a otro, con la finalidad de obtener un beneficio económico para sí o para un tercero, manipule un sistema informático, mediante la introducción, alteración, daño o supresión de datos informáticos o a través de cualquier interferencia en el funcionamiento de un sistema informático, será penado:"

1.1. *Actividad típica*

El verbo rector del tipo es "manipular". La RAE ha definido manipular como "Operar con las manos o con cualquier instrumento"[29]. A su vez, existe una segunda definición que puede ser relevante, dado que este mismo ente también define a el verbo como "intervenir con medios hábiles y, a veces, arteros, en la política, en el mercado, en la información, etc., con distorsión de la verdad o la justicia, y al servicio de intereses particulares"[30]. Por lo tanto, al menos en los términos relevantes para este asunto, la manipulación se refiere a la intervención sobre algún objeto, con el propósito de distorsionarlo de una forma tal, que el objeto resultante sea uno distinto al que era previo a la manipulación.

Ahora bien, este tipo permite distinguir dos modalidades: una estricta y otra amplia. La primera modalidad es la estricta, en la cual la manipulación se debe realizar a través de medios de ejecución ya determinados por la LDI. que son la introducción, alteración, daño o supresión de datos informáticos.

La introducción es la acción y efecto de introducir o introducirse, mientras que introducir equivale a meter o hacer entrar, en este caso, los datos en el sistema informático

[29] RAE, Diccionario de la lengua española, s. v. «manipular», primera acepción
[30] RAE, Diccionario de la lengua española, s. v. «manipular», tercera acepción.

afectado. En segundo lugar, la alteración es la acción de alterar, comportamiento que puede entenderse como cambiar o modificar la configuración de los datos del sistema informático de que se trate. Más concretamente, la doctrina española entiende por alteración "toda perturbación funcional definitiva", que podría verificarse añadiendo nuevos datos, borrando parcialmente los existentes, eliminando o modificando las relaciones entre ellos. En tercer lugar, dañar es el efecto de dañar, comportamiento que se identifica con causar un detrimento, perjuicio o menoscabo a dichos datos. Finalmente, la supresión: es la acción y efecto de suprimir, conducta que puede equipararse a la de eliminar los datos en cuestión[31].

Se entiende que es un delito con los medios de ejecución vinculados y que basta que la manipulación del sistema informático a través de cualquiera de estas hipótesis para que se consume el delito. En esta misma línea, Mayer y Vera afirman que *"la manipulación referida puede verificarse a través de cinco modalidades alternativas, de modo que basta que se verifique cualquiera de ellas para que se configure el delito de fraude informático del art 7° inciso primero de la nueva ley"*[32].

Por otra parte, en la modalidad amplía la manipulación se puede realizar a través de cualquier interferencia indebida en el sistema informático. A diferencia de la estricta, no se establecen medios específicos por la cual se deba realizar esta manipulación. Además, esta misma puede afectar cuál función del sistema informático, a diferencia de lo que sucede con el tipo presente en el artículo 468 del Código penal, lo cual se tratará más adelante.

Si bien es innegable que el tipo de la LDI se inspiró en lo dispuesto por el Convenio de Budapest, existen diferencias entre ellos. En el convenio de Budapest, se establece que se debe castigar tanto la generación de perjuicio patrimonial a través de la introducción, alteración, borrado o supresión de datos informáticos o la intromisión indebida en el sistema informático, siendo dos hipótesis diferentes. En cambio, en la LDI lo que se castiga específicamente es la "*manipulación de sistemas informáticos, mediante la introducción, alteración, daño o supresión de datos informáticos"*. El uso de la palabra "mediante" indicaría que aquí los datos informáticos son solamente un medio para conseguir la manipulación del sistema. Esta es una observación relevante, ya que provocaría que, al menos para este tipo, la *"manipulación de datos informáticos"* no pueda tenerse como equivalente a la *"manipulación de sistemas informáticos"*. La redacción del tipo deja bastante claro que el uso de los datos informáticos sólo supone uno de los dos medios posibles que el legislador establece para conseguir la manipulación de los sistemas informáticos.

[31] Mayer-Vera, "La nueva Ley de delitos informáticos", *Revista de Ciencias Penales,* sexta época, vol. XLVIII, N.º 3, 2022, p. 152.
[32] Vera Vega, Jaime y Mayer Lux, Laura**.** *Delitos informáticos y cibercriminalidad: aspectos sustantivos y procesales*. 1 vol. Editorial B de F, Ciudad Autónoma de Buenos Aires, 1ª ed. 2024, tomo único, p. 273.

Finalmente, esta manipulación del sistema debe ser relevante. Tal como deja en claro Hernández, la manipulación implica necesariamente una intervención que altere su normal funcionamiento, quedando excluidas las conductas que, aunque desleales o de cualquier modo ilícitas, no impliquen una distorsión funcional[33]. Por lo tanto, la manipulación debe ser de tal entidad, que, con la alteración del funcionamiento provocada, permita afirmar que el sistema informático previo a la manipulación difiere del sistema posterior a ella.

Respecto al resultado, la redacción del tipo lleva a la inequívoca conclusión de que el resultado requerido por el delito es un perjuicio patrimonial, del cual depende la pena[34], provocando que este tipo sea un delito de resultado.

Sin embargo, Hernández hace una observación muy interesante que es necesario traer a colación. Esta observación sugiere la posibilidad de que, debido a la redacción del tipo, en la cual el gerundio *"causando perjuicio a otro,* el perjuicio cumpliría una función adverbial. Lo anterior provocaría que ésta constituya una circunstancia concomitante de la conducta y no necesariamente el resultado perseguido objetiva y subjetivamente por ella, lo que a su vez podría llevar a concluir que este es una condición objetiva de punibilidad y no necesariamente el resultado del delito.[35]

Una condición objetiva de punibilidad es un elemento de una ley penal cuya satisfacción es presupuesto de la punibilidad de una conducta, pero que no el objeto de una imputación subjetiva. Por lo tanto, respecto de estos elementos no debe analizarse ni el dolo ni la imprudencia, ni la culpabilidad"[36]. En consecuencia, si es que se adhiere a esta postura, no queda más que concluir que el monto del perjuicio no es un elemento del tipo que deba estar abarcado por el dolo del autor . Sin embargo, la interpretación más adecuada es aquella que adhiere a la tesis de que el perjuicio patrimonial es el resultado y no una condición objetiva de punibilidad. El problema con la segunda hipótesis es que al asumir que el perjuicio es una condición objetiva de punibilidad, este no debe estar abarcado por el dolo del autor, provocando una situación de responsabilidad objetiva que debería ser evitada por una interpretación conforme a la Constitución[37].

---

[33] Hernández, M., "La esperada consagración de un genuino delito de fraude informático en el Derecho penal chileno (art. 7º de la Ley nº 21.459)", en Bascur Retamal, G. y Letonja Cepeda, T. (eds.), *Delitos Informáticos*, DER Ediciones, Santiago de Chile, 2025, p. 220.

[34] Va de presidio menor en su grado mínimo y multa de cinco a diez unidades a presidio menor en su grado máximo y multa de veintiuna a treinta unidades tributarias mensuales, dependiendo del monto de perjuicio.

[35] Hernández, M., "La esperada consagración de un genuino delito de fraude informático en el Derecho penal chileno (art. 7º de la Ley nº 21.459)", en Bascur Retamal, G. y Letonja Cepeda, T. (eds.), *Delitos Informáticos*, DER Ediciones, Santiago de Chile, 2025, p. 221.

[36] Kindhäuser, Urs y Zimmermann, Till. *Derecho penal. Parte general*. 1 vol. Tirant lo Blanch, Valencia, 1.ª ed. 2024, tomo único, p. 100

[37] Hernández, M., "La esperada consagración de un genuino delito de fraude informático en el derecho penal chileno (art. 7º de la Ley nº 21.459)", en Bascur Retamal, G. y Letonja Cepeda, T. (eds.), *Delitos Informáticos*, DER Ediciones, Santiago de Chile, 2025, p. 221.

1.2 Objeto material

El objeto material de un delito es el objeto real sobre el cual se lleva a cabo la acción típica[38]. Ahora bien, su determinación no supone un ejercicio interpretativo tan complejo como la determinación del bien jurídico de este mismo. Este es siempre fácil de establecer mediante la interpretación gramatical del tipo.[39]

Lo que se tipifica específicamente es la generación de un perjuicio, a través de la manipulación de *un sistema informático.*

En general, la doctrina está conteste de que el objeto material del fraude informático son los datos informáticos[40]. Sin embargo, no es posible afirmar esto al menos respecto del tipo de la LDI. Aquí la manipulación no recae sobre datos informáticos, recae sobre los sistemas informáticos. El mismo tipo es bastante claro al establecer que se castiga al que "manipule sistemas informáticos", siendo los datos informáticos un de los posibles medios por los cuales conseguir dicha manipulación.

La misma LDI ha definido a los sistemas informáticos como "todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa."

Esta definición es bastante similar a la entregada por la informática, que define los sistemas informáticos como "el conjunto de elementos físicos y lógicos (computadores, monitores, teclados, ratones, impresoras, personas, etc.) que, mediante la explotación de aplicaciones informáticas, y de forma coordinada y cooperativa, permiten resolver un problema dado"[41].

Por lo tanto, tanto la LDI como la informática entienden que los sistemas informáticos son los dispositivos físicos utilizados para la resolución de problemas mediante la explotación de aplicaciones informáticas. La manipulación debe recaer sobre ellos. El tipo prescribe que se castiga la manipulación de sistemas informáticos *"mediante"* la introducción, alteración, daño o supresión de datos informáticos". Dado que se usa la preposición "mediante", la cual es definida por la RAE como "por medio de"[42], está claro que los datos informáticos son un medio para conseguir conseguir la misma, y no son el objeto de esta.

---

[38] Jescheck, Hans-Heinrich, *Derecho Penal. Parte General*, Comares Berlín, 2002, p. 277.
[39] Mayer, Max Ernst, *Derecho penal. Parte general*, B de F , Buenos Aires, 2007, p. 122.
[40] En esta línea Mayer-Calderón, "El delito de fraude informático: Concepto y delimitación", Revista chilena de Derecho y tecnología, VOL. 9 N°. 1, 2020; Hernández, M., "La esperada consagración de un genuino delito de fraude informático en el derecho penal chileno (art. 7º de la Ley nº 21.459)"; Bascur Retamal, Gonzalo y Letonja Cepeda, Thommas, *Delitos Informáticos*, DER Ediciones, Santiago de Chile, 2025.
[41] Castrillón Santana, Modesto Fdo., et al., *Fundamentos de informática y programación para ingeniería*, Paraninfo, Madrid, 2011, p. 4.
[42] RAE, Diccionario de la lengua española, s. v. «mediante», primera acepción.

1.3 Aspectos subjetivos

En este caso, el tipo requiere que el perjuicio se cause con la finalidad de obtener un beneficio económico, ya sea propio o para un tercero. Aquí es evidente que se trata de un elemento subjetivo del tipo, referido al ánimo de lucro, y basta con que concurra en el momento de la ejecución de la conducta. Además, para la consumación del delito basta con que el agente actúe con esta finalidad y no es necesario la obtención de esta.

1.4 *Iter Criminis*

Al ser un delito de resultado, admite formas de ejecución imperfectas de la conducta, es decir, tentativa y consumación.

1.5 Autoría y participación

El inciso final del artículo 7° de la LDI establece que *"para los efectos de este artículo se considerará también autor al que, conociendo o no pudiendo menos que conocer la ilicitud de la conducta descrita en el inciso primero, facilita los medios con que se comete el delito."*

Esta disposición fue agregada en el primer trámite constitucional por la Comisión de Seguridad Pública del Senado, a instancia del Ministerio Público, para cubrir la situación de las personas que facilitan sus cuentas como destino de transferencias ilícitas.[43]

Esta es una regla especial de participación, según la cual se equipara una forma de complicidad con la autoría. En cuanto a la exigencia "conociendo o no pudiendo menos que conocer la ilicitud de la conducta", tiene varias interpretaciones en la doctrina chilena.

La expresión "conociendo o no pudiendo menos que conocer" no es nueva, y ha sido incorporada anteriormente en otros delitos y acepta varias interpretaciones.

En primer lugar, Hernández sostiene que en este caso se trataría de una participación imprudente en un delito doloso."*Lo realmente novedoso, y especialmente controversial, sería que se entendiera que, contra lo que sugiere la primera lectura, la fórmula aludiera a una culpa stricto sensu, con lo cual se configuraría un caso inédito de participación imprudente en un delito doloso, con la misma pena no solo de la participación dolosa, sino también de la autoría dolosa"* [44]. Sin embargo, esta interpretación resulta inadecuada, dado que nuestro Código penal establece un régimen de numerus clausus respecto de la responsabilidad penal por delitos culposos, limitándola únicamente a los supuestos expresamente previstos por la ley. Considerando que el inciso en cuestión no hace

[43] Historia de la Ley 21.459, pág 120.
[44] Hernández, M., "La esperada consagración de un genuino delito de fraude informático en el Derecho penal chileno (art. 7º de la Ley nº 21.459)", en Bascur Retamal, G. y Letonja Cepeda, T. (eds.), *Delitos Informáticos*, DER Ediciones, Santiago de Chile, 2025, pág 228.

referencia alguna a la imprudencia, negligencia o infracción de reglamentos, puede concluirse que no se configura una hipótesis de participación culposa.

La segunda postura sostiene que, en todos los casos en que la ley establece este tipo de exigencias, se consagran hipótesis de responsabilidad objetiva. En esta línea, Guzmán Dalbora concluye que *"estamos ante un delito de sospecha; más aún, que aquí la ley ha remachado una responsabilidad objetiva que, según mi modesto entender, resiste a pie firme cualquier interpretación culpabilista y constituye una ominosa supervivencia penal en el Código"*.[45] Se trata de una crítica legítima y acertada a la lógica subyacente en estas disposiciones, pero que no da una propuesta a cómo este tipo de disposiciones deben ser interpretadas y aplicadas en nuestro sistema jurídico.

La tercera tesis propone una interpretación más garantista. Parte de la premisa de que el artículo 1° del Código penal establece una presunción general de dolo[46]. Desde esta perspectiva, la expresión "no pudiendo menos de conocer" sería una exigencia probatoria destinada a hacer inaplicable dicha presunción. Sin embargo, esta postura debe ser rechazada, pues implicaría admitir que el artículo 1° contiene una presunción de dolo, lo que resulta incompatible con el principio de culpabilidad.

La cuarta tesis, planteada por Ossandón, entiende esta expresión como una manifestación de la normativización del dolo. Las teorías que siguen esta línea coinciden en que la realidad debe concebirse de forma valorativa y no meramente empírica, ya que lo relevante para el Derecho penal no es lo que el sujeto efectivamente se representa, sino el conocimiento que le era exigible. De este modo, el dolo se convierte en un asunto normativo de exigibilidad, por lo que no todo error excluye responsabilidad. Así, se considera que el sujeto actúa con dolo cuando el conocimiento de los hechos le era exigible[47].

Finalmente, una quinta tesis rechaza la anterior, argumentando que esta emplea un concepto de dolo distinto al utilizado en el resto del ordenamiento jurídico chileno. Según esta posición, la fórmula no implica renunciar al componente cognoscitivo del dolo, sino advertir sobre la posibilidad de invocar errores inverosímiles o situaciones de desconocimiento que no resulten reales[48].

Otro punto que puede resultar problemático, es la extensión de lo que el sujeto debe conocer. En este caso no se hace referencia a un aspecto específico, tal como lo hace el

---

[45] Guzmán Dalbora, Luz y sombras en La "nueva" disciplina de la receptación, en *Colectánea criminal, estampas de la parte especial del Derecho penal,* Editorial B de F, Buenos Aires, 2017, pág 101-129

[46] Novoa, E., *Curso de Derecho Penal chileno*, Tomo I, Edit. Jurídica de Chile, Santiago, 1960, p. 502

[47] Ossandón Widow, M., "El delito de receptación aduanera y la normativización del dolo", *en Revista Ius et Praxis*, año 14, núm. 1 (2008), pp. 49–86

[48] González Lillo, D., "El delito de receptación: Bien jurídico ofendido y problemas de imputación subjetiva a la luz del artículo 456 bis A del Código penal chileno", en *Pro Jure Revista de Derecho*, Pontificia Universidad Católica de Valparaíso, vol. 63 (2024): pp. 315–348.

Código penal[49] o la Ordenanza de Aduanas[50] en la receptación. Aquí se exige el conocimiento de la ilicitud de la conducta, por lo que al menos en un inicio, lo que se exige es el conocimiento de la antijuricidad de la conducta y no solo de los requisitos típicos de esta[51].

2° El fraude informático del Código penal: actividad típica, objeto material, elementos subjetivos de lo injusto

Posteriormente, el año 2023 se publica la Ley 21.595, que sistematiza los delitos económicos. Esta ley contempla delitos propios y modifica diversos cuerpos legales. Esta ley agrega un nuevo inciso en el artículo 468 del Código penal, el cual contempla nuevamente un tipo de fraude informático. Al parecer, este tipo viene a cumplir la función de tapar un vacío legal que existe respecto de la estafa, tal como se deja ver en la historia de ley[52].

Este nuevo artículo 468, tipifica al fraude informático de la siguiente manera:

"Las penas del artículo anterior serán aplicadas también al que para obtener un provecho para sí o para un tercero irrogue perjuicio patrimonial a otra persona:

1. Manipulando los datos contenidos en un sistema informático o el resultado del procesamiento informático de datos a través de una intromisión indebida en la operación de éste."

2.1 Actividad típica

En este nuevo tipo, el verbo rector sigue siendo "manipular", por lo que respecto a la extensión de las conductas captadas por este podemos remitirnos a lo dicho anteriormente en lo relativo al fraude informático de la LDI. Sin embargo, es menester resaltar que en este caso, no existen medios de ejecución vinculados, por lo tanto, la manipulación se podría realizar de cualquier manera.

2.2 Objeto material

---

[49] Artículo 456 BIS A *"El que conociendo su origen o no pudiendo menos que conocerlo, tenga en su poder, a cualquier título, especies [...]"*

[50] Artículo 182 *" Las penas establecidas por los delitos de contrabando o fraude se aplicarán también a las personas que adquieran, reciban o escondan mercancías, sabiendo o debiendo presumir que han sido o son objeto de los delitos a que se refiere este Título"*.

[51] Hernández, M., "La esperada consagración de un genuino delito de fraude informático en el Derecho penal chileno (art. 7º de la Ley nº 21.459)", en Bascur Retamal, G. y Letonja Cepeda, T. (eds.), *Delitos Informáticos*, DER Ediciones, Santiago de Chile, 2025, p. 228.

[52]"*El académico señor Héctor Hernández señala que este artículo complementa la tipificación de la estafa, superando un sensible vacío respecto del delito de estafa o fraude informático.*"Historia de la Ley N° 21.595, p 156.

Si bien inicialmente se puede pensar que la redacción de los tipos es idéntica, la verdad es que un análisis profundo permite concluir que existen diferencias sustanciales. Y es en este plano, el del objeto material, en que estas se manifiestan.

El tipo de fraude informático presente en el artículo 468 del Código penal tipifica la manipulación de datos informáticos o la de sistemas informáticos, cuando la manipulación afecta a la capacidad de procesamiento de datos.

Por lo tanto, la manipulación debe recaer directamente sobre los datos informáticos o el resultado de procesamiento informático de datos. En consecuencia, aquí también se pueden distinguir dos hipótesis.

En la primera, se manipulan datos informáticos que están contenidos en un sistema informático. Aquí el objeto material del delito no son los sistemas informáticos, sino los datos contenidos en él. Por otro lado, en la segunda hipótesis, lo que se manipula sigue siendo el sistema informático. Sin embargo, lo que debe resultar afectado por la manipulación es una función específica, la del procesamiento informático de datos. Por lo que, al menos según la redacción del tipo, las intromisiones indebidas en un sistema informático, que afecten a funciones distintas de la mencionada anteriormente, como la de almacenamiento o la de representación informática de datos, serían atípicas respecto de este tipo.

Como se dijo anteriormente, la LDI establece varias definiciones importantes, siendo una de ellas la de ***datos informáticos***. Específicamente, el articulo 15 de la LDI define datos informáticos como: "*toda representación de hechos, información o conceptos expresados en cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función"*.

La relación de la informática con los datos es tan estrecha que la misma palabra informática proviene de una expresión francófona, que se obtiene de contraer las palabras information y automatique.[53] La definición actual de la informática es "conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de computadoras"[54].

Para la ciencia informática, los datos son *"un conjunto de símbolos utilizados para expresar o representar un valor numérico, caracteres, un hecho, un objeto o una idea. Todo dato debe siempre representarse de forma adecuada para poder ser objeto de tratamiento automático"*[55]. Este último aspecto es muy relevante, ya que las computadoras en su estado esencial no pueden captar todo tipo de información.

[53] Castrillón Santana, Modesto., et al, op. cit., pág 1.
[54] RAE, Diccionario de la lengua española, s. v. «informática», tercera acepción.
[55]Castrillón Santana, Modesto., et al, op. cit., pág 13.

La tecnología utilizada por los sistemas informáticos, incluso los más avanzados, a su nivel esencial sólo distingue dos estados: encendido y apagado. Esto último se debe a que los computadores almacenan la información utilizando el sistema de numeración binario, donde cualquier dato o información debe ser transformado o codificado a este sistema. En este sistema binario existen dos símbolos, "1" y "0". Cada dígito recibe el nombre de bits y constituye el nivel de información más fundamental. Ahora bien, para representar un carácter es necesario al menos 8 bits, lo que corresponde a un byte.

El proceso mediante el cual se traspasa información de un formato determinado a otro, se conoce como codificación. Esta codificación se debe realizar de tal manera, que eventual permita realizar el proceso inverso en cual se transforma la información de binario a su forma original. Este proceso se conoce como decodificación[56].

Ahora bien, la forma en que se codifica la información depende en gran medida de qué tipo de entidades se trate. En general, se pueden distinguir cuatro tipo de entidades: texto y valores alfanuméricos, valores numéricos, sonidos e imágenes.

En cuanto a la representación de los primeros dos, es la más sencilla. La representación valores de texto, tales como letras, símbolos, números, de control[57], se realiza mediante la traducción de aquellos a un conjunto de bits, cuya cantidad necesaria varía según el número de caracteres distintos que se quiera representar [58]. Sin embargo, la representación de valores numéricos para la realización de operaciones aritméticas es un poco más compleja, y varía según si el número que se busca representar es entero o uno decimal, pero en el fondo supone un procedimiento similar.[59]

Respecto al sonido, este se digitaliza después de que las ondas sonoras sean captadas por un micrófono. Mientras mayor sea la frecuencia de muestreo, más fiel será la representación del sonido de manera digital ya que se realizan más tomas de muestras por segundo. La operación para que el sistema informático pueda guardar este tipo de información sonora, supone que se transforme estas ondas sonoras en bits.[60]

Finalmente, existen dos formas para representar imágenes en computadoras, los mapas de bits y los gráficos vectoriales. Los primeros suponen entender la imagen como un rectángulo, el cual se divide por muchas rejillas rectangulares pequeñas, conocidas como píxeles. Los píxeles de una imagen se almacenan en memoria de forma consecutiva empleando un número de bits para representar el valor de cada píxel. Mientras más de estos tenga la imagen (resolución) y mientras mayor sea el número de bits por píxel, mayor calidad tendrá la imagen. Por otro lado, la imagen vectorial se describe como "una

[56] Ídem págs 13-36.
[57] Por ejemplo, el espaciado.
[58] Por ejemplo, la letra "a" en binario se representa como "01100001".
[59] Castrillón Santana, Modesto., et al, op. cit., pág 27 -34.
[60] Ídem cfr pág 34

colección de objetos, tales como líneas, polígonos y textos con sus respectivos atributos o detalles, modelados por medio de vectores y ecuaciones matemáticas que determinan su forma como su posición dentro de la imagen[61].

Por lo visto hasta ahora, lo que la informática entiende por dato coincide perfectamente con la definición que entrega la LDI. Podemos observar que todo lo que se puede representar en un sistema informático, coincide con la definición establecida en la LDI en cuanto a "*toda representación de hechos, información o conceptos expresados en cualquier forma que se preste a tratamiento informático"*. Sin embargo, existe una diferencia fundamental, ya que además de lo anterior, la LDI también considera datos informáticos "*los programas diseñados para que un sistema informático ejecute una función"*.

La informática define programa como un conjunto ordenado de instrucciones que se suministra a la computadora indicando las operaciones o tareas que se desea que se realice. A su vez, las instrucciones son un conjunto de símbolos pertenecientes a un repertorio que representa una orden de operación o tratamiento para la computadora, por ejemplo, suma, multiplica, lee de teclado, etc. [62] Normalmente las instrucciones vinculadas a los datos que puede ejecutar un procesador son de transferencia, tratamiento y bifurcación.

A su vez, los programas están estrechamente relacionados con el software. El último es el conjunto de elementos lógicos que dotan al hardware de un sistema informático de la capacidad para realizar algún tipo de trabajo o tarea de manera automática. Por lo tanto, el software es el conjunto de instrucciones que indican al ordenador lo que tiene que hacer. Se entiende que este software está compuesto por un gran número de programas.

Por otro lado, se pueden distinguir dos tipos de software, el software del sistema y el software de aplicaciones. El primero está compuesto por el conjunto de programas imprescindibles para el funcionamiento del hardware, más un conjunto de utilidades cuya misión es facilitar el uso del sistema y optimizar sus recursos, sistemas operativos etc. Mientras que el segundo, es el conjunto de programas que maneja el usuario para realizar cualquier tarea con el sistema informático, aplicaciones ofimáticas, diseño gráfico, software a medida etc.

No obstante, la LDI solo hace una referencia genérica a "*programas diseñados para que el sistema informático ejecute una función"*, y no hace ninguna especificación respecto a qué tipo de programa se refiere. Es fundamental tener en cuenta esta diferenciación realizada por la informática, ya que es relevante para una interpretación sistemática basada en el tenor literal de la Ley. Lo anterior se debe a que, sin esta diferenciación, se podría suponer que la manipulación de cualquier programa contenido en un sistema informático

[61] Ídem cfr pág 34.-35
[62] Ídem cfr pág 77.

terminaría siendo una manipulación de datos informáticos. Esto convertiría en trivial a cualquier esfuerzo enfocado en diferenciar los "datos informáticos" de los "sistemas informáticos" como objetos materiales del delito de fraude informático. Ahora bien, este esfuerzo recobra sentido y utilidad si se tienen en cuenta esta diferencia evidencia por la informática[63].

Teniendo en cuenta la distinción entre software del sistema y software de aplicación, se podría concluir que cuando la manipulación recae en la BIOS, el cargador, la interfaz de usuario o el sistema operativo[64] se están manipulando sistemas informáticos. Esto es porque, al manipular esta clase de programas lo que se está afectando es el funcionamiento del sistema informático. Esto ocurre, porque al manipular dichos elementos, se hace posible distinguir el sistema previo de la manipulación al resultante de esta. Por otro lado, cuando la manipulación recae sobre programas que pueden ser considerados como software de aplicación, como procesadores de texto, hojas de cálculos electrónica, gestor de bases de datos, gráficos o comunicaciones, lo que se está manipulando son datos informáticos. Una manipulación de este tipo de programas no afecta al funcionamiento del sistema informático, al menos de una manera esencial. Por ejemplo, si se hackea un determinado programa instalado en una computadora, que tenga la función de procesar datos para realizar operaciones matemáticas para determinar cuál debe ser el valor de un determinado producto, no se está afectando el funcionamiento de la computadora en el cual está instalado. La computadora sigue funcionando igual que lo hacía antes del hackeo de su programa, no afecta a sus otras funciones ni tampoco a las otras aplicaciones, lo único afectado es el programa manipulado.

Por lo tanto, a pesar de que la LDI incluya los programas dentro de los datos informáticos, un análisis detallado teniendo en cuenta las distintas clasificaciones presentes en la informática, permite determinar que el objeto material, al menos en la primera hipótesis de manipulación informática del artículo 468 del Código penal, son los datos informáticos. Respecto a la segunda modalidad de este artículo, es decir aquella en la cual la intromisión indebida afecta al procesamiento informático de datos, se da cuando se manipula programas de software que tengan la función de procesar datos informáticos.

2.3 Aspectos subjetivos

[63] En esta línea, en España por ejemplo,también se distingue entre el delito de daños a sistemas y datos informáticos en el artículo 264 de su Código penal.Artículo 264. 1. El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años. 2. Se impondrá una pena de prisión de dos a cinco años y multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias: 1.ª Se hubiese cometido en el marco de una organización criminal. 2.ª Haya ocasionado daños de especial gravedad o afectado a un número elevado de sistemas informáticos.[...]". Por lo tanto, Chile no sería el único país en el cual un mismo delito informático tenga diferentes objetos materiales.

[64] Todos estos son programas que forman parte del "software de sistema".

En este caso el tipo también requiere que la manipulación que se cometa con la finalidad de obtener un beneficio para sí mismo o para un tercero. Sin embargo, una diferencia que podría ser relevante respecto al tipo de la LDI es que, en este, se establece expresamente que ese beneficio buscado perseguido debe ser uno de carácter económico. Sin embargo, entendiendo que este delito se encuentra ubicado en el párrafo de las defraudaciones, mediante una interpretación sistemática con las otras disposiciones, podemos concluir que aunque no lo mencione expresamente, este beneficio debe ser de carácter económico. Finalmente, dado que se requiere un elemento subjetivo de lo injusto, al menos en un inicio, este delito se podría cometer solo con dolo directo.

2.4 Iter criminis

Al ser un delito de resultado, admite formas de ejecución imperfectas de la conducta, es decir, tentativa y consumación.

3° Bien jurídico protegido en el fraude informático.

Aunque la definición de bien jurídico ha sido muy discutida desde el nacimiento del concepto, actualmente la mayoría de la doctrina entiende que estos son intereses individuales o colectivos, juzgados indispensables para la vida en sociedad.[65] Si bien la doctrina ha intentando establecer varias distinciones entre los bienes jurídicos, tales como los bienes jurídicos intermedios[66], en general se distinguen dos tipos, que se clasifican de acuerdo al titular de estos. En esta línea, se distinguen los bienes jurídicos individuales, cuyo titular es una persona individual y determinada, de los colectivos, cuyo titular es el conglomerado social.[67]

Se entiende que la determinación del bien jurídico protegido por un delito es fundamental desde un punto de vista dogmático, y cumple cuatro funciones: la primera es una función sistemático-clasificatoria, en cuya virtud es posible ordenar el estudio de los tipos de la Parte especial. Por otro lado, y particularmente, constituye un criterio rector de la categoría sistemática de la tipicidad como ámbito de significado y valoración. En tercer lugar, es un elemento muy relevante para la interpretación teleológica de los tipos[68]. Finalmente, adquiere importancia como parámetro para el establecimiento de penas proporcionales.

Ahora bien, este ejercicio dogmático adquiere una doble relevancia en el fraude informático. Esto es porque el bien jurídico de este delito se puede analizar entendiéndolo

---

[65] Politoff, Sergio, Matus, Jean Pierre y Ramírez, María Cecilia, *Lecciones de Derecho Penal chileno. Parte general. Segunda edición actualizada*, Jurídica de Chile, Santiago de Chile, 2004, p. 67

[66] Corcoy, *"Delitos de peligro y protección de bienes jurídico-penales supraindividuales",* editorial B de F, 2024, p. 215.

[67] Hormazabal, Consecuencias político criminales y dogmáticas del principio de exclusiva protección de bienes jurídicos, *"Revista de Derecho",* Vol XIV, 2003, p. 129.

[68] Silva Sánchez, *Derecho Penal. Parte General*, Civitas , Cizur Menor (Navarra), 2025, pág 202.

como una defraudación o como un delito informático. Sin embargo, esto último requiere un paso previo, que supone analizar si es que realmente el fraude informático es un delito informático.

Esto en un inicio es problemático, porque actualmente no existe consenso sobre lo que debemos entender por delito informático. Las primeras definiciones de delitos informáticos eran bastantes simples, y los entienden como la "la criminalidad mediante computadoras"[69] .

Sin embargo, existen definiciones más completas. Mayer distingue criminalidad informática en sentido amplio y en sentido estricto. La primera es "la criminalidad cometida mediante sistemas informáticos" y suele utilizarse para referir la comisión de delitos tradicionales a través de computadoras o de internet. Mientras que, en su sentido estricto, es aquella cometida en contra de sistemas informáticos, y suele emplearse para aludir a comportamientos delictivos que inciden, directamente, en un sistema informático[70].

A pesar de que el concepto propuesto anteriormente supone un gran avance respecto al primero, no goza de una aceptación unánime en la doctrina chilena. Navarro crítica la posición anterior, aludiendo a que esta es una distinción que se fundamentada en una legislación derogada, que ofrecía una regulación demasiado amplia de "delitos informáticos", y que lo anterior explicaba la necesidad de crear un concepto ideal o abstracto de delito informático, como el concepto estricto mencionado anteriormente. Es por lo que, basándose en la nueva Ley 21.459 , propone una nueva forma de definir los delitos informáticos. Ahora, esta nueva definición no encuentra su sustento en el objeto material de estos delitos, sino en el nivel de vinculación de la conducta con los medios informáticos. Según esta teoría existen tres niveles de vinculación[71]:

En un primer nivel, el más débil de los tres, tal tecnología puede ser meramente contingente: aunque el tipo penal no la considere en absoluto, ella podría ser empleada en su ejecución como un instrumento de apoyo.

En el segundo nivel de vinculación, la tecnología informática aparece como accesoria. En este caso, la descripción abstracta del tipo que efectúa la Ley no requiere que la conducta sea ejecutada con ayuda de tales tecnologías, pero su utilización por parte del sujeto activo produce como efecto una potenciación de sus efectos dañinos.

Finalmente, el tercer nivel de vinculación, el más fuerte de los tres, la tecnología informática aparece como esencial. En este caso, el legislador ha descrito una conducta

---

[69] TIEDEMANN, "Criminalidad Mediante Computadoras", *en Nuevo Foro Penal N° 30*, octubre/diciembre 1985, p. 481.

[70] Mayer, "El Bien Jurídico en los delitos informáticos", Revista Chilena de Derecho, vol. 44 Nº 1, 2017. p. 237.

[71] Navarro, "El concepto de delito informático según la nueva legislación chilena (Ley N.º 21.459)". *Revista de política criminal*. Vol. 18 N.º 36. diciembre 2023, p. 674.

cuya ejecución requiere necesariamente la utilización de tecnología informática, de modo que una conducta específica en la que ella no se emplee, no tiene posibilidad alguna de realizar el tipo

Si analizamos la pertenencia de los delitos informáticos desde la perspectiva de la clasificación de Mayer, podemos concluir que el fraude informático pertenece a la criminalidad informática en el sentido estricto. A pesar de que el fraude informático fue tipificado con la idea de que sirviera de complemento a la estafa, la verdad es que es un delito completamente diferente. Es erróneo afirmar que el fraude informático es una estafa que se comete mediante sistemas informáticos. La estafa como tal, requiere que exista una conducta engañosa, que haga a otra persona recaer en un error, para que realice un acto de disposición que cause un perjuicio patrimonial. Esto requiere que necesariamente exista una interacción entre dos personas, dado que el engaño y el error son fenómenos psicológicos que solo se pueden dar en la mente de las personas naturales. Por otro lado, el fraude informático se puede dar sin que exista interacción entre las personas. Para realizar este último se requiere necesariamente una manipulación que afecte al sistema informático, es decir, una que se realice en contra de estos, ya sea manipulando directamente al sistema o a los datos informáticos que se contengan en él. Por lo tanto, el fraude informático es un delito que solo se puede cometer utilizando sistemas informáticos, por lo que encajaría dentro de la criminalidad informática informática en sentido estricto.

En cambio, si utilizamos la clasificación propuesta por Navarro, el fraude informático se encuentra en el tercer nivel. Utilizando los mismos argumentos que se dieron anteriormente, queda claro que el fraude informático es un delito donde la tecnología es esencial, dado que el delito exige manipulación de datos o sistemas informáticos, lo que no se puede realizar sin tecnología.

Ahora bien , respecto al bien jurídico en los delitos informáticos, existen tres posturas que son especialmente relevantes. La primera alude a que, en este tipo de delitos, no existe ningún bien jurídico que sea exclusivamente protegido por ellos. La segunda postula que los delitos informáticos protegen un bien jurídico diferente de los bienes jurídicos tradicionales. La última es una posición ecléctica ya que combina aspectos de las tesis anteriores.

Como se dijo anteriormente, la primera tesis postula que en los delitos informáticos sólo se protegen bienes jurídicos tradicionales. Por lo tanto, quienes se adhieren a esta postura, afirman que lo "informático" de estos delitos, no es más que un contexto delictivo o un particular medio de afectación a bienes jurídicos tradicionales[72]. Entre estos delitos sólo existiría una diferencia de forma y no de fondo, ya que los intereses afectados serían idénticos en ambos casos. Esto se vería reflejado en el sabotaje y fraude informático, ya

[72] Mata "Delitos cometidos mediante sistemas informáticos (estafas, difusión de materiales pornográficos, ciberterrorismo", *Cuadernos Penales José María Lidón,* Universidad de Deusto, N.º 4, 2007, pp. 129-171.

que serían delitos que tienen como bien jurídico protegido la propiedad y el patrimonio respectivamente[73].

Al contrario de la postura anterior, quienes defienden esta postura afirman que los delitos informáticos resguardan un bien jurídico distinto del protegido por los delitos tradicionales. Por lo tanto, entre delitos informáticos y tradicionales existiría una diferencia de fondo y no de forma.

Dentro de esta postura existen varios planteamientos. El primero de ellos postula que el bien jurídico tutelado por los delitos informáticos es la calidad, pureza e idoneidad de la información contenida en un sistema informático[74]. Esta se basa en la Ley 19.223 , ya que en la moción parlamentaria que la originó se afirma que se busca proteger este nuevo interés. Sin embargo, esto es rápidamente descartable, porque estas son expresiones sin una connotación técnica y un sentido natural obvio, además que difícilmente pueden ser consideradas un bien jurídico. Este último debe ser concreto, delimitable y socialmente relevante, características que no se cumplen en conceptos tan vagos e indeterminados. En segundo lugar, dentro de las funciones de legislador no se encuentra declarar que bienes jurídicos protege cada delito. Esta misión de determinación lo tiene la dogmática penal y se debe realizar a través de un detallado análisis de cada disposición, plantear que el bien jurídico protegido es tal porque lo declaró el legislador es un error, que se basa en la errada ficción originada en el siglo XVIII según la cual de que el legislador es siempre racional[75] .

La segunda postura relevante, alude a que el bien jurídico protegido por los Delitos Informáticos es el software[76] como objeto de tutela penal. Esta postura, nace de una moción producida en la discusión de la Ley. "*Sin embargo, la Comisión y el autor de la moción tienen una concepción distinta. Sostienen que el "software", en sí mismo, constituye un bien jurídico en el mundo moderno que requiere de protección jurídica, más allá de si se le utiliza como elemento para cometer un delito. En derecho penal hay diversos bienes jurídicos que se protegen: la vida, la propiedad, el honor, la familia. Aquí se incorpora un bien jurídico nuevo, el sistema automatizado de información conocido como "software"*"[77]. Sin embargo, de lo razonado en cuanto al objeto material de ambos tipos de fraude informático, podemos concluir que esta tesis es errónea, en cuanto confunde el objeto material de los delitos informáticos con el bien jurídico.

La tercera postura plantea al internet como objeto de tutela penal. Sin embargo, esta es rechazada por tres razones. En primer lugar, porque la protección penal de internet no permite superar la abstracción y amplitud atribuidas a la tutela de la información. En

[73] Vera Vega, Jaime y Mayer Lux, Laura, *Delitos informáticos y cibercriminalidad. Aspectos sustantivos y procesales*, B de F, Buenos Aires, 2024, p. 90.
[74] Historia de la Ley N° 19.223 pág 3.
[75] Zaffaroni, *Manual de derecho penal. Parte general*, Editorial Ediar, Buenos Aires, 2ª ed., 2006, pág. 345.
[76] Sin embargo, la Comisión y el autor de la moción tienen una concepción distinta. Sostienen que el "so
[77] Historia de la Ley 19.233, pág 31.

segundo lugar, la protección punitiva de internet parece confundir el contexto de comisión de un delito con el bien jurídico tutelado por él. Finalmente, porque la tutela penal de internet no toma en cuenta que muchos de los delitos informáticos se pueden cometer sin internet[78].

Ahora bien, también existen quienes aluden que la confianza en el correcto funcionamiento de los sistemas informáticos es el bien jurídico protegido por estos delitos. El problema de esta postura es que Derecho penal solo puede proteger algo que ya existe, lo que excluiría a la confianza, la cual existiría sólo porque así lo dispone una norma jurídica. La confianza en la conducta de otras personas sería una mera suposición acerca de cómo se espera que ellas se comporten. Por último, la confianza es afectada por el delito cuando este queda sin sanción[79].

Finalmente, la postura que tiene más aceptación es aquella que sugiere que el bien jurídico de los delitos informáticos es la funcionalidad informática como interés que surge respecto de redes computacionales. Este es un presupuesto para la realización de diversas actividades de gran relevancia para las personas y las instituciones que están a su servicio en un Estado democrático de Derecho. Estas actividades resultan relevantes por motivos cuantitativos -la cantidad de actividades que se realizan- y cualitativos -la índole de esas actividades-. La funcionalidad informática es el conjunto de condiciones que posibilitan que los sistemas informáticos realicen adecuadamente las operaciones de almacenamiento, tratamiento y transferencia de datos, dentro de un marco tolerable de riesgo. Ella constituye, por otra parte, un bien jurídico instrumental de carácter colectivo, cuya tutela penal debe verificarse en términos particularmente acotados, dado que sirve a otros intereses penalmente relevantes y no es posible castigar todas las actividades que inciden en un sistema informático que no son capaces de afectar actividad de relevancia para las personas. Es por esto que solo se afecta a este bien jurídico cuando para la comisión del delito se utilicen redes computacionales o internet. Por otro lado, al servir a la generalidad de las personas y ser un interés cuyo disfrute no es exclusivo de ningún individuo, se le considera un bien jurídico colectivo.

Este último planteamiento es el que parece más adecuado, en cuanto al bien jurídico de los delitos informáticos, dado que supera los problemas de abstracción . Sin embargo, al menos respecto del fraude informático no se puede plantear que solo protege un interés exclusivamente informático. De la tipificación del fraude informático, tanto en el Convenio de Budapest como en el Derecho positivo chileno, podemos concluir que es un delito de lesión patrimonial; más precisamente, puede ser interpretado como un delito en que el

[78] Mayer. "El bien jurídico en los delitos informáticos", *Revista Chilena de Derecho*, vol. 44, Nº 1, 2017, cfr págs 242-243.
[79] Vera Vega, Jaime y Mayer Lux, Laura, *Delitos informáticos y cibercriminalidad. Aspectos sustantivos y procesales*, B de F, Buenos Aires, 2024, cfr págs 100-103.

perjuicio patrimonial de otro es ocasionado a través de determinados medios informáticos[80]. Por lo tanto, si bien es posible aceptar que el fraude informático tutele a la funcionalidad informática, no lo hace de manera exclusiva, ya que además de esta también custodia intereses patrimoniales. El principal argumento para afirmar lo anterior, está en que ambos tipos de fraude informático exigen daño patrimonial para su consumación, variando su penalidad. Es menester mencionar que nosotros debemos entender que aquí el concepto de patrimonio coincide con el planteado por las posturas mixtas, es decir, como el conjunto de cosas u otras entidades dotadas de valor monetario y unidas a su titular por un vínculo jurídicamente reconocido o con apariencia de tal[81].

Rivacoba en su monografía sobre el contrato simulado da la siguiente definición de defraudación: "por defraudaciones debe entenderse todos aquellos ilícitos en que se emplee el fraude, o, quizás mejor, producidos o logrados mediante fraude. A su vez, dice del fraude lo siguiente: "tomando en consideración lo genuino de esta manera de obrar que es el fraude, en sus dos modalidades, y su oposición a la actividad física o corporal del agente, resulta lógico definirlo como medio o modo de obrar engañoso o abusivo de confianza de que se sirve una persona para obtener un resultado antijurídico y en concreto en los delitos contra los derechos patrimoniales, para causar a otro un daño económico y estimable en dinero, tipificado penalmente"[82]. A su vez, Quintano Ripollés destacaba que lo esencial en las es la relación causa y efecto entre el ánimo de lucro y el resultado patrimonial lesivo, a través de la acción fraudulenta típica[83]. Finalmente, la voz "fraude" también se utiliza como sinónimo de defraudación, esto es, no para aludir al medio de provocación del perjuicio, sino que el perjuicio mismo.

Es en esta línea que , suele distinguirse entre fraudes por engaño, fraudes por abuso de confianza, fraudes impropios o llevados a cabo por medios distintos del engaño o del abuso de confianza, fraudes regulados en leyes especiales etc[84]. En todos esos casos, los términos "fraude "y "defraudación "son intercambiables, de suerte que también puede aludir a defraudaciones por engaño. Sin embargo, esta distinción entre fraudes propios e impropios no parece adecuada, en cuanto el adjetivo "impropio" generalmente se utiliza para forzar la inclusión de conceptos en categorías a la cual no pertenecen realmente.

Aun así, el fraude informático, efectivamente puede ser considerado una defraudación. Esto porque, al menos en la doctrina, lo importante de las defraudaciones es que constituyan medios inmateriales que sirvan para obtener un resultado antijurídico,

[80] Mayer-Calderón, "El delito de fraude informático: Concepto y delimitación", *Revista chilena de Derecho y tecnología*, VOL. 9 N°. 1, 2020, p. 170.
[81] Oliver Calderón, G., "Delitos contra la propiedad", en Rodríguez Collao, L. (coord.), *Derecho penal. Parte especial.* Volumen II, Editorial Tirant lo Blanch, España, 2022, p. 215.
[82] Rivacoba, El delito de contrato simulado, Akal, Madrid, 1992, pp. 11-32.
[83] Quintano Ripollés, A. Tratado De La Parte Especial Del Derecho Penal. Segunda Edición. Vol II Madrid 1972, págs 200 y ss
[84] Mayer, *Delitos económicos de estafa y otras defraudaciones*, DER EDICIONES, Santiago, 2018, p. 20

consistente en una disminución del patrimonio del sujeto pasivo, siendo esto lo que precisamente ocurre con este delito.

Finalmente, es menester mencionar que nosotros debemos entender que aqui el concepto de patrimonio coincide con el planteado por las posturas mixtas, es decir, como el conjunto de cosas u otras entidades dotadas de valor monetario y unidas a su titular por un vínculo jurídicamente reconocido o con apariencia de tal.[85]

Por lo tanto, el fraude informático no entra en la definición clásica de defraudación, ya que no se realiza mediante el engaño o el abuso de confianza. Sin embargo, esto no ha sido impedimento para que otras conductas que tampoco entren en estas dos categorías sean consideradas defraudaciones. Lo anterior permite concluir que el fraude informático sí cumple las condiciones para ser una defraudación impropia, porque en la regulación que se le ha dado, efectivamente hay una conducta que se realiza con ánimo de lucro, causando un perjuicio patrimonial del sujeto pasivo a través de medios inmateriales.

En conclusión, el fraude informático se erige como una figura delictiva compleja que eventualmente protege una pluralidad de bienes jurídicos, fusionando la tutela de intereses colectivos e individuales. No es posible considerar que sea un delito que atenta exclusivamente contra la funcionalidad informática, dado que su tipificación, al exigir un perjuicio en el patrimonio de un tercero, lo convierte en un delito patrimonial. Además, de acuerdo a lo planteado anteriormente, los delitos informáticos sólo lesionan la funcionalidad informática cuando se cometen a través de redes computacionales o internet. Así, el fraude informático es un tipo que protege especialmente el patrimonio dado que para su consumación exige un perjuicio patrimonial avaluable en dinero. Sin embargo, puede puede convertirse en un delito pluriofensivo, cuando la vulneración de la seguridad del sistema se comete por los medios anteriormente mencionados. Sin embargo, dado que el uso de redes computacionales o internet para cometer fraudes informáticos es algo común, mas no esencial[86], no es posible afirmar que es un pluriofensivo en todos los casos.

4° Conclusiones preliminares

Al analizar dogmáticamente los tipos de fraude informático, se puede concluir que al menos en sus aspectos medulares, ambos tipos son extremadamente similares, ya que en ambos la fisonomía típica de ambos radica en radica en el medio empleado para menoscabar el patrimonio ajeno, esto es, la manipulación o alteración indebida de datos informáticos o sistemas informáticos, básicamente, dada por la intromisión directa por medios informáticos en un patrimonio ajeno[87]. Específicamente, en LDI se tipifica la

[85] Oliver Calderón, G., "Delitos contra la propiedad", en Rodríguez Collao, L. (coord.), Derecho penal. Parte especial. Volumen II, Editorial Tirant lo Blanch, España, 2022, p. 215.
[86] En el sentido de que se puede cometer este delito sin recurrir a internet o a estas redes computacionales.
[87] Bascur Retamal, Gonzalo y Letonja Cepeda, Thommas, *Delitos Informáticos*, DER Ediciones, Santiago de Chile, 2025. cfr págs 120-124.

manipulación de un sistema informático, ya sea con el uso de datos informáticos o con cualquier interferencia en su funcionamiento. En la otra vereda, el Código penal castiga la manipulación en los datos contenidos en un sistema informático o en el sistema mismo, solo que afectando su capacidad de procesamiento de datos.

Por otro lado, a pesar de las semejanzas estructurales entre ambos tipos, se pueden identificar diferencias sustanciales que ocasionan que estos no estén en una relación de igualdad absoluta en el plano lógico semántico.

La primera de ellas se manifiesta en el objeto material del delito. En cuanto al objeto material, el tipo de fraude informático de la LDI, se concluye que este es el "sistema informático". Se llega a esta conclusión, en cuanto a la redacción del tipo castiga al que *"manipule un sistema informático"*. La conducta típica, es decir, la manipulación, debe recaer sobre dichos sistemas. En cambio, en el fraude informático del Código penal la manipulación debe recaer en "los datos contenidos en un sistema informático" o en la capacidad de procesamiento de datos del sistema.

Esta distinción entre datos y sistemas informáticos está sustentada normativamente tanto por la LDI como conceptualmente por la ciencia informática. Los datos informáticos son la representación de hechos, información o conceptos, de forma tal que estos sean susceptibles al tratamiento informático. Mientras que los sistemas informáticos son aquellos aparatos que permiten dicho procesamiento. La diferenciación no es baladí ni fruto de un ejercicio dogmático que no tiene aplicación práctica. En realidad, es perfectamente diferenciable la manipulación de sistemas y datos informáticos. La primera se produce cuando se manipula lo que se conoce como "software del sistema", programas esenciales como el BIOS o el sistema operativo, cuya alteración provoca un cambio de funcionamiento de magnitud en el sistema. Este debe ser de tal magnitud que no sea posible afirmar que el sistema previo a la manipulación sea el mismo al resultante de esta. A su vez, la segunda se produce cuando se manipula información o programas no esenciales contenidos en un sistema informático. En estas situaciones, la manipulación de información o programas no afectan al funcionamiento del sistema, sino a la aptitud funcional propia de estos.

Ahora bien, a pesar de que el tipo del Código penal también contempla una hipótesis de manipulación sobre el sistema informático, esta es diferenciable de la prevista en la LDI. En el artículo 468 se castiga la manipulación del sistema cuando esta recae sobre una función específica de este, la del procesamiento de datos. Lo anterior provoca que, cuando la manipulación que afecte a un sistema informático recaiga sobre una función distinta del procesamiento informático de datos, esta será típica para el artículo 7 de LDI y no el 468 del Código penal, dado que este contempla la manipulación cuando afecta la capacidad de procesamiento de datos del sistema.

La segunda diferencia se manifiesta en el ámbito de los medios de ejecución. En el artículo 7° de la LDI se tipifica un delito con los medios de ejecución vinculados. Estos se corresponden con la introducción, alteración, daño y supresión de datos informáticos. Además, en este mismo artículo se contempla una modalidad amplia, según la cual la manipulación se puede cometer mediante cualquier intervención que afecte al normal funcionamiento del sistema. Por su parte, el artículo 468 del Código penal no vincula ningún medio de ejecución, por lo cual la manipulación de datos y del procesamiento informático de estos se puede realizar de cualquier forma.

En tercer lugar, se observa una sutil diferencia en los aspectos subjetivos del tipo. En la LDI se exige que el delito sea cometido con la finalidad de obtener un beneficio económico para sí mismo o para un tercero. Mientras que, el Código penal sólo establece que se debe perseguir la obtención de un beneficio, no especificando el carácter de éste.

Finalmente, en relación con el objeto de protección, puede afirmarse que el fraude informático constituye un delito de carácter complejo, cuyo bien jurídico tutelado admite un análisis desde una doble perspectiva: como un delito informático o como una defraudación.

Si analizamos esta modalidad de fraude como un delito informático, podemos concluir que este, eventualmente, tutela lo que se denomina “funcionalidad informática”. Esta protección es eventual, en cuanto la lesión solo se produce cuando los delitos informáticos se producen en el contexto de un ataque a redes computacionales o mediante internet. Esto se debe a que, al ser un bien jurídico instrumental, su protección debe ser acotada. Por lo anterior, y a pesar de que estas condiciones son importantes para el desarrollo de la sociedad, sólo resultan perjudicadas cuando un gran número de sistemas informáticos se ven afectados. Por lo tanto, un razonamiento congruente con lo planteando que la tesis que afirma que los delitos informáticos tienen como bien jurídico la “funcionalidad informática”, debería concluir que cuando se manipula un sistema informático de forma aislada, no se lesiona o se pone en peligro a este bien jurídico.

Por último, si analizamos este delito como una defraudación, es evidente que este es un delito que tutela al patrimonio como un bien jurídico. Que el bien tutelado sea el patrimonio se hace evidente cuando, en ambos tipos de fraude informático, se exige un perjuicio patrimonial estimable en dinero para su consumación. Por otro lado, se puede considerar que el fraude informático es una defraudación, porque es un delito que utiliza medios inmateriales para producir un perjuicio patrimonial.

Relaciones concursales del fraude informático de la Ley 21.459 y el del artículo 468 del Código penal.

1° Vigencia simultánea de estas defraudaciones o derogación tácita de la precedente en el tiempo.

La derogación es "la cesación de la vigencia de una ley en virtud de la disposición de otra ley posterior. Importa privar a la primera de su fuerza obligatoria, reemplazando sus disposiciones por otras"[88]. En el artículo 52 del Código civil, se reconocen dos clases, la expresa y la tácita. A su vez, estas pueden ser totales o parciales.

De acuerdo a este artículo, la derogación expresa se produce cuando la nueva ley menciona explícitamente que deroga la anterior. Un ejemplo de este tipo de derogación lo podemos encontrar precisamente en la LDI. Este cuerpo normativo, específicamente, su artículo 17, establece que "sin perjuicio de lo dispuesto en el artículo primero transitorio de esta ley, derógase la ley N° 19.223. Toda referencia legal o reglamentaria a dicho cuerpo legal debe entenderse hecha a esta ley." .

Se entiende que la derogación expresa se realiza en virtud de una potestad normativa, es decir, la atribución de crear, alterar o eliminar normas, que es conferida a una persona o grupo de personas, por una regla o un complejo de estas. Precisamente, el efecto de esta es la pérdida de vigencia de la norma, entendiendo esto último como la eliminación de la norma del ordenamiento jurídico. Si se analiza desde la perspectiva de la teoría de la legislación, cuando se deroga una ley, existe una disposición operativa -un enunciado fijado por el legislador que contiene actos de establecimiento, modificación o supresión de normas- , contenida en un texto autoritativo, que termina con la vigencia de una disposición normativa[89]. En este caso, la disposición autoritativa es el artículo 17 de la LDI, mientras que la disposición normativa derogada, es la Ley 19.223 en su conjunto. En conclusión, dado que en la Ley 21.595, no contiene ninguna disposición que derogue de manera manifiesta al artículo 7° de la LDI, este último no ha sido derogado expresamente por la reforma prevista en la Ley 21.595.

Podríamos arribar a la misma conclusión mediante la figura de la derogación tácita, en la medida en que se ha establecido que ambos tipos penales se aplican a supuestos fácticos distintos, dado que contemplan objetos materiales diferentes. Por ello, no puede sostenerse que la nueva ley contenga disposiciones incompatibles con las de la anterior, lo

[88] ALESSANDRI-SOMARRIVA, *Derecho civil. Parte preliminar y parte general* (Explicaciones basadas en las versiones de sus clases, redactadas, ampliadas y actualizadas por Antonio Vodanovic H., 5ª edición, Santiago, 1990), t. I, p. 190.

[89]Bascuñan A., "Sobre la distinción entre derogación expresa y derogación tácita", en *Anuario de filosofía jurídica y social*, núm. 18, cfr págs 230-236.

que impide afirmar que el fraude informático previsto en la LDI haya sido derogado por el nuevo tipo de fraude informático incorporado en el Código penal.

Sin embargo, existe otra forma de analizar a la institución de la derogación tácita. Según Bascuñan, la derogación expresa opera de una forma distinta a la derogación tácita . La primera se vale de mecanismos que provocan la pérdida de vigencia de una norma determinada, mientras que la segunda, es una forma de aplicación de un criterio de solución de antinomias de primer grado, concretamente, del criterio que da preferencia a lex posteriori respecto de la lex priori[90]. Esta se extiende a todas las disposiciones que resulten incompatibles con la Ley nueva, por lo tanto, si una Ley establece penas distintas penas para un delito que estaba regulado en una Ley anterior, se entiende que esta última se encuentra derogada tácitamente.

En consecuencia, la derogación tácita no requiere una disposición operativa en un texto autoritativo. Es fruto del ejercicio interpretativo de los órganos jurisdiccionales, por lo que es constatada o declarada cuando estos determinan qué norma debe ser aplicada con preferencia a otra en un caso determinado, por lo que resuelve problemas de *aplicabilidad* y no de vigencia. Es por esto que en ningún momento se cuestiona la vigencia de la norma anterior, dado que esta es un presupuesto operatividad de esta forma de derogación. "Aunque la lex posteriori haya entrado en vigencia después que la lex priori, ambas se encuentran simultáneamente vigentes al momento de entrar en una antinomia"[91].

"El mero carácter sucesivo de las normas no puede fundamentar por sí mismo la derogación"[92]. Por lo tanto, para determinar si el artículo 468° del Código penal -Ley posterior- deroga tácitamente al artículo 7° de la LDI -Ley anterior-, se debe analizar si estas dos normas se encuentran en conflicto. Se entiende que la derogación tácita presenta características que exigen mucha cautela en su aplicación, pues, a diferencia de la derogación expresa, en la cual no hay problemas para determinar cuál norma se deroga, en la derogación tácita debe seguirse un procedimiento de estudio e interpretación destinado a establecer un proceso y, dentro de ellas, qué disposiciones deben estimarse derogadas[93].

Existe un conflicto entre normas cuando *"estamos en presencia de un conflicto de normas toda vez que en un mismo ordenamiento jurídico coexistan dos normas que regulan una conducta de manera incompatible"*[94] o "*cada vez que exista* inconsistencias *entre dos o más normas"*[95].

---

[90] Bascuñan A., "El principio de lex mitior ante el Tribunal Constitucional ", *Revista de Estudios de la Justicia,*en, núm. 23, 2015,cfr p 16.
[91]Ídem, p 5.
[92] Gascón, M, "Cuestiones sobre la derogación", C*uadernos de Filosofía del Derecho*. núm. 15-16, vol. II (1994), p 855.
[93] Oliver Calderón, G., "*Retroactividad e irretroactividad de las leyes penales"*, Editorial Jurídica de Chile, Santiago de Chile, 2007, p. 38.
[94] Squella Narducci, *Introducción al derecho*, 7ª ed., Thomson Reuters, Santiago de Chile, 2022, P. 409.
[95] Ídem, p 407.

Por lo tanto, entendiendo a la derogación tácita como el resultado de un ejercicio interpretativo, que busca resolver un problema de aplicación normativa , el primer paso para determinar si existe un conflicto entre el art 7° de la LDI y el 468 del Código penal, debería ser si estas son aplicables a los mismos casos. Y en segundo lugar, en caso que la respuesta a la primera pregunta sea positiva, se debería determinar si la norma aplicable se decide de acuerdo al principio lex posterior derogat legi anteriori.

Partiendo de lo establecido en el capítulo anterior, hay que entender que ambos tipos suponen una alteración funcional de datos o sistemas informáticos, la cual provoca un mal funcionamiento en estos. Estos tienen el mismo verbo rector, que es "manipular", por lo que, en un inicio, sería aplicable a los mismos casos. Sin embargo, tal como se concluyó en el capítulo anterior, existe una diferencia esencial que provoca ,una aplicación diferencia de estas normas Esta diferencia está en el objeto material de los delitos: el artículo 468 del Código penal castiga la manipulación de datos informáticos, mientras que el artículo 7° de la LDI hace lo mismo, pero con la manipulación de sistemas informáticos. Por lo tanto, debido al hecho de que estas normas no son aplicables a los mismos casos, este conflicto normativo no es uno que pueda ser resuelto mediante la derogación tácita de uno de los tipos. Además sería importante tener en cuenta que existen autores que proponen "si el conflicto se produce entre el criterio de especialidad y el cronológico, debe ser resuelto a favor del primero de ellos, de modo que *lex posterior non derogat priori speciali"*[96].

Por lo tanto, dado que las normas se aplican a situaciones diferentes, no se puede afirmar que el fraude informático introducido al ordenamiento jurídico chileno por la Ley 21.595 haya derogado al fraude informático previsto en el artículo 7° de la LDI.

2° Problemas concursales del fraude informático y determinación del concurso aparente de leyes o concurso de delitos

2.1 Problemas concursales del fraude informático en general

El fraude informático es un delito que comporta diversos problemas concursales, ya que se encuentra muy relacionado, sea con delitos informáticos, sea con delitos comunes.

En primer lugar, el fraude informático se encuentra vinculado con conductas que no son causa directa del perjuicio, pero que sí son necesarias para conseguir datos indispensables para provocarlos. Por ejemplo, con el phishing en su segunda etapa de desarrollo, ya que este último puede ser constitutivo del delito de acceso ilícito. La diferencia es que el fraude informático requiere un ánimo de lucro, mientras que el acceso ilícito no.

En segundo lugar, también está relacionado con el sabotaje informático, ya que ambos se pueden realizar a través de la afectación de datos informáticos. Sin embargo, al

[96] Ídem. p 417.

igual que en el caso anterior, se diferencian porque el fraude requiere ánimo de lucro, mientras que el sabotaje no

El vínculo entre el fraude informático y la estafa resulta evidente. No obstante, la estructura típica del fraude informático difiere sustancialmente de la de la estafa, lo que se aprecia en los elementos constitutivos de cada figura. En la estafa se requiere un engaño que genere un error, el cual motive un acto de disposición patrimonial y, como consecuencia, produzca un perjuicio económico, todo ello unido por una relación de causalidad. El error, al ser un fenómeno psicológico, no puede ser atribuido a las máquinas[97]. Por esta razón, no es posible sancionar como estafa las conductas fraudulentas «respecto de» o «contra» sistemas automatizados de tratamiento de información. Tales conductas se enmarcan, en cambio, dentro del ámbito del fraude informático.

Una relación menos evidente es la que se establece entre el fraude informático y el hurto. Por regla general, en el ámbito de los delitos informáticos se vincula el hurto con conductas como la usurpación de identidad. Sin embargo, el vínculo que aquí se plantea considera el hurto en su sentido más básico: como figura fundamental de los delitos de apropiación. Esta conexión surge si interpretamos el hurto en un sentido inmaterial, entendido por algunos autores como la ruptura de una cadena de custodia y la creación de una nueva. Desde esta perspectiva, su dimensión conceptual adquiere relevancia, lo que dificulta diferenciar ambos ilícitos. Así, si se concibe el hurto de manera inmaterial, la transferencia de fondos mediante la manipulación de una página bancaria podría parecer un caso de hurto. No obstante, ello no es correcto, pues, como señala Hernández, el objeto material de ambos delitos es distinto: el hurto recae sobre "una cosa corporal mueble ajena", mientras que el fraude informático tiene por objeto, al menos aparentemente, "datos informáticos", que carecen de corporalidad[98].

Finalmente, existe una relación entre el fraude informático y el uso fraudulento de tarjetas de pago y transacciones electrónicas. La diferencia entre ambos delitos se da porque , la conducta regulada en el uso de tarjetas indebidas exige o engaño o simulación, lo que lo acerca más a las conductas de estafa y phishing, lo cual implica interacción entre personas. Sin embargo, en los delitos informáticos en sentido estricto no es necesaria interacción alguna[99].

2.2 Determinación del concurso aparente de leyes o concurso de delitos

---

[97] Politoff-Matus-Ramírez, Lecciones de derecho penal chileno: Parte especial, Editorial Jurídica de Chile, Santiago, 2005, p. 412.

[98] Hernández, "La esperada consagración de un genuino delito de fraude informático en el Derecho penal chileno (Art 7° de la Ley N° 21.459)" en Scheechler (edit) Riveros (coord.) L*os delitos informáticos: Aspectos político-criminales, penales y procesales en la ley n° 21.459,* DER EDICIONES, Santiago de Chile, 2024, p. 214.

[99] Mayer -Calderón, op. cit., p. 168.

Entendiendo que el art 468 del Código penal no derogó tácitamente al artículo hay que determinar si entre ellas existe un concurso de delitos o un concurso aparente de leyes penales.

La estructura del concurso de delitos, por regla general, se aborda mediante la distinción entre concurso real de delitos y concurso ideal de delitos. El primer tipo de concurso se da cuando una pluralidad de hechos punibles se juzga en el mismo procedimiento o se somete a una posterior formación de una pena global o conjunta[100]. Por otro lado, el concurso ideal implica la unificación de varias infracciones a la ley en un solo hecho al que se le fija una sola pena[101]. De acuerdo con el artículo 75 del Código penal, el concurso ideal solo supone la unidad de hecho y no de acción, ya que hay tipos que exigen una pluralidad de acciones para consumar el hecho[102].

El primer concurso a descartar es el real . La aseveración anterior se fundamenta en primer lugar, en que estos tipos tienen una aplicación diferenciada. Tal como se ha concluido anteriormente, si bien ambos delitos tienen una estructura típica similar, existen discrepancias que provocan que estos tengan una aplicación[103].

Un segundo motivo para descartar este tipo de concurso, es que la aplicación de este violaría el principio non bis in idem. La regla non bis in idem aparece formulada en el diccionario compilado por Liebs como ne bis in idem (crimen iudicetur), cuya traducción literal es como sigue: "que no se sentencie dos veces por un mismo delito[104]. Aplicar las penas previstas por ambos tipos a una sola manipulación informática significaría una vulneración a este principio, ya que un mismo hecho se castigaría dos veces, incurriendo en una duplicidad sancionadora que el ordenamiento jurídico rechaza. La esencial del concurso real es la existencia de una pluralidad de hechos o al menos de resultados, situación que aquí no existiría.

Un tercer motivo para rechazar la aplicación de un régimen de concurso real, que se deriva del anterior, es la vulneración del principio de proporcionalidad. Este principio supone una prohibición del exceso en el marco de la duración de una sanción determinada[105], por lo tanto se vulnera cuando se conmina una pena excesiva en relación con su gravedad[106]. Imponer las penas de ambos delitos significa una vulneración de este principio, supondría la aplicación de una pena acumulativa, desproporcionada frente a la unidad de acción que caracteriza el caso.

---

[100] Roxin, Derecho Penal: Parte General, Thomson Reuters-Civitas, Navarra, 1ª edición, t. II, p 981.
[101] Kindhäuser, Urs y Zimmermann, op. cit., p 698.
[102] Cury, *Derecho penal: parte general*, Ediciones universidad católica de Chile, Santiago de Chile, 8 ed, 2005, cfr págs 663-666.
[103] El análisis más preciso sobre que tipo se debe aplicar a cada hipótesis se realizará en el siguiente apartado.
[104] Barja de Quiroga, *El principio non bis in idem*, Editorial Dykinson, Madrid, 2004, p. 14.
[105] Roxin, *Derecho Penal: Parte General,* Thomson Reuters-Civitas, Navarra, 1ª edición, t. I, p 103.
[106] Silva Sanchez op., ed. et vol. cits., pág. 382.

Por otro lado, el concurso ideal debe ser igualmente descartado. Si bien es cierto que un inicio, al menos en apariencia, cumple el supuesto del concurso ideal (un hecho que vulnera varias disposiciones), un análisis detallado permite concluir que esto no es así. Para fundamentar esta posición se pueden utilizar los mismos argumentos que fueron entregados para descartar el concurso real, es decir[107].

Sin embargo, a estos argumentos se puede adicionar uno que es fundamental, y es que en este caso no se aprecia una doble lesión de bienes jurídicos, la cual es un fundamento jurídico esencial del concurso ideal. Este tipo de concurso sólo se justifica cuando mediante un solo hecho se infringen dos o más disposiciones, lesionando dos o más bienes jurídicos, sin que exista un tipo capaz de cubrir penalmente ambas lesiones[108]. Tal como se analizó en el capítulo anterior, la estructura típica de los delitos analizados revela una homogeneidad en su redacción y finalidad , lo que permite concluir que ambos tutelan el mismo bien jurídico: el patrimonio y eventualmente la funcionalidad informática.

Este punto es crucial porque, si no hay diversidad de bienes jurídicos, desaparece la razón de ser del concurso ideal. La aplicación de esta figura en el caso concreto implicaría una duplicidad normativa sin justificación material, generando un incremento punitivo que carece de sustento en la teoría del bien jurídico y que vulneraría el principio de proporcionalidad.

En conclusión, entre ambos tipos no existe una relación de concurso de delitos sino un concurso aparente de leyes penales.

3° El concurso aparente de leyes entre el fraude informático de la Ley 21.459 y el del artículo 468 del Código penal.

"Con respecto al concepto básico, existe acuerdo amplio. Como es sabido, se admite que hay concurso de leyes cuando, según el texto de la ley, pueden aplicarse a una acción por lo menos dos tipos legales pero, en vista de la relación que existe entre las disposiciones legales que están en juego y en las cuales están determinados los correspondientes tipos, resulta que sólo puede aplicarse un tipo legal"[109].

Estas reglas resuelven las relaciones entre las diferentes disposiciones penales, de modo que la aplicabilidad de unas se condiciona con la aplicabilidad o no aplicabilidad de otras. Este tipo de concurso nace porque a veces es preciso trazar reglas para saber cuando una disposición consiste o excluye la contemporánea o sucesiva aplicación de otras. Por lo tanto, esta es una institución sustantiva que se ubica dentro del campo de la interpretación

[107] Estas son: las normas tienen una aplicación diferenciada y vulnera los principios de non bis in idem y proporcionalidad.
[108] Novoa, E., *Curso de Derecho Penal chileno*, Tomo II, Edit. Jurídica de Chile, Santiago, 1960, cfr p 231.
[109] Klug, "Sobre el concepto de concurso de leyes", *en Problemas fundamentales de la filosofía y de la pragmática del derecho*, Barcelona-Caracas: Alfa, 1989, p 55.

frente a una situación de hecho[110]. Los principios que se utilizan para determinar la preferencia de la aplicación de un tipo sobre otro son los de especialidad, consunción, alternatividad o subsidiariedad.

El primero de ellos es el de especialidad. Dos tipos penales tienen una relación de especialidad cuando un precepto penal contiene conceptualmente todas las características de otro precepto, de modo que la realización del tipo delictivo especial también satisface de modo inevitable el respectivo tipo general[111]. Los supuestos de aplicación de este principio podríamos representarlos con dos círculos concéntricos, siendo el precepto especial el de menor diámetro[112]. Esta es la relación que se da, por ejemplo, entre el homicidio y el parricidio. Este último contiene todos los elementos del primero, pero agrega un elemento, relativo a la exigencia del vínculo de sangre (y su conocimiento) entre el sujeto activo y pasivo del delito. Por lo tanto, cuando hay especialidad todos los casos que se subsumen bajo la norma especial se podrían subsumir también bajo la norma general, pero esta última alcanza al menos un caso adicional[113].

Se entiende que en el caso de la especialidad, la Ley general es desplazada por la Ley especial por razones lógicas[114]. Lo anterior no está expresado en lugar alguno del Código, pero se deduce de la misma existencia de los preceptos especiales, que no tendría razón de ser si fueran de aplicación las generales[115].

El segundo tipo de relación en que se pueden encontrar es la de subsidiariedad. Los concursos aparentes de leyes penales por subsidiariedad serían aquellos en que la relación entre dos preceptos legales por lo menos un caso concreto que es subsumible en uno de dichos preceptos lo es también en el otro, y por lo menos un caso concreto que es subsumible en lo primero no lo es en el segundo, y viceversa, pues ambos preceptos tienen en común al menos una propiedad o elemento del tipo relevante, aunque ninguno es especial o general respecto del otro[116]. Este es una forma de evitar que la no concurrencia de determinados requisitos deje sin sanción un hecho que, de todos modos, puede ser sancionado por otro precepto que no exige estos requisitos[117]. Por lo tanto la ley subsidiaria se aplicará en defecto de la ley principal.

---

[110] Jiménez de Asúa,. *Tratado de Derecho Penal*, Editorial Losada. S. A,Buenos Aires , 1950, t II, cfr págs 535-562.
[111] Wessels, Beulke y Satzger. *Derecho penal. Parte general: el delito y su estructura*. Instituto Pacífico, Lima, 1.ª ed., 2018, p. 551.
[112] Cerezo Mir,, *Derecho penal. Parte general*, B de F, Buenos Aires, 2008, p. 1037.
[113] Van Weezel, *Curso de derecho penal. Parte general*, Ediciones UC, Santiago, 1.ª edición, 2023, p. 499.
[114] Mezger, *Derecho penal: parte general*, Editorial Bibliográfica Argentina S. R. L., Buenos Aires, 1958, p. 346.
[115] Antón Oneca, *Derecho penal parte general,* 2a. ed., Akal, Madrid, 1986, p. 495.
[116] Mattus Ramirez, *Manual de Derecho penal chileno:* parte general, Tirant lo Blanch, Santiago de Chile, 2ed, 2021, p.564.
[117] Muñoz Conde y Mercedes García, *Derecho Penal. Parte General*, Editorial Tirant lo Blanch, 11ª edición, 2022 p. 490.

A su vez, parte de la doctrina distingue entre la subsidiariedad formal o expresa, donde esta misma está expresamente prevista por la ley y los casos de subsidiariedad material o tácita, donde la subsidiariedad tiene que ser derivada por la interpretación del autor. Sin embargo, hay un sector de la doctrina que sólo reconoce la existencia de la subsidiariedad expresa[118], al definir a la subsidiariedad como "hay concurso aparente y no concurso ideal de delitos cuando un hecho pareciera ser captado por dos tipos, pero, por *expresa disposición de la ley,* uno de ellos resulta desplazado, porque su aplicación se subordina precisamente a que el otro no concurra[119].

Un ejemplo de subsidiariedad expresa se puede encontrar en el artículo 481 del Código penal, "El que fuere aprehendido con artefactos, implementos o preparativos conocidamente dispuestos para incendiar o causar algunos expresados en este párrafo, será castigado [...] **salvo que pudiendo considerar el hecho como tentativa de un delito determinado debiera castigarse con una pena mayor**" . En la última parte de este inciso el legislador deja clara la relación de subsidiariedad.

Ahora bien, en los ejemplos de subsidiariedad tácita reconocidos por la doctrina, generalmente hay una conexión entre los tipos. Por ejemplo, en el caso del artículo 445 del Código penal : " el que fabricare, expendiere o tuviere en su poder llaves falsas, ganzúas u otros instrumentos destinados conocidamente **para efectuar el delito de robo** [...]" . Aquí hay una conexión, ya que el tipo dice "para efectuar el delito de robo".

La tercera regla del concurso aparente de leyes penales es la de consunción o absorción. Estamos en casos de consunción en todos aquellos supuestos en que, no siendo apreciable una relación de especialidad o subsidiariedad, se rechaza el tratamiento concursal común, porque uno de los preceptos concurrentes regula un hecho que sólo puede considerarse como acceso o meramente acompañante, en sentido. amplio, del que regula el precepto principal que lo desplaza[120]. Siguiendo la misma línea, según estos autores estaríamos frente a estos casos, por ejemplo, "Los que consisten en actos preparatorios especialmente punibles con relación a la tentativa y a la consumación del delito preparado"[121]. A lo anterior, se puede agregar la definición de consunción de Hellmuth Mayer "El tipo consumido es un medio habitual cuando no indispensable de la realización" la cual es traída a colación por Klug en su análisis sobre el concepto de concurso de leyes[122].

Por lo tanto, su característica principal estriba en que una disposición absorbe a la otra (lex consumens derogat legi consumptae). Ello se debe a que los valores que contienen

---

[118] Esto se origina en Etcheberry quien no utiliza la distinción entre subsidiaridad expresa y tácita, en Etcheberry, *Derecho penal: parte General,* Editorial Jurídica, Santiago, 3ed, 1998, t II, pág 127.
[119] Cury op. cit., p. 670.
[120] Cury op. cit., p 565.
[121] Idem, p. 566.
[122] Klug, *Problemas de la filosofía y de la pragmática del derecho*, Fontamara, Coyoacán, 2002, pág 60.

no son equivalentes como en la alternatividad, ni auxiliar uno de otro como en la subsidiariedad, sino superior el de una de ellas, cuya superioridad es tan clara que al aplicar el artículo absorbente se realiza de modo completo, por la mayor importancia del tipo y de la pena, la misión sancionadora que se efectúa en nombre de las dos disposiciones: la que consume y la consumida[123]. Esta sería precisamente una manifestación de la dimensión material del non bis in idem, ya que "no pueden aplicarlo los dos tipos penales porque uno de ellos "absorbe" por completo el desvalor del otro, de tal manera que el desvalor que representa este último se puede considerar "copenado" al castigar el primero. Desde el otro punto de vista: frente al otro tipo pena, el que no se aplica aparece como insignificante"[124].

Al analizar las distintas definiciones sobre este tipo de concurso, se concluye que para que exista una relación de consunción entre dos tipos penales es necesario que uno represente un mayor desvalor que el otro. Esto se debe a que, según esta regla, un tipo se aplica en lugar del otro porque el primero absorbe el desvalor del segundo. Por ello, la diferencia de desvalor entre los tipos es condición indispensable para aplicar esta forma de resolución del concurso aparente de leyes penales. No puede existir consunción entre dos tipos con desvalor equivalente, ya que ninguno podría absorber al otro.

La cuarta regla relevante para resolver concursos aparentes de leyes penales es la alternatividad. Se entiende que existe este tipo de relación entre dos preceptos cuando estos contemplan un mismo hecho desde distintos puntos de vista, de manera que o bien resultan idénticos o se comportantes como dos círculos secantes que tienen una zona común, pero no están comprendidos el uno en el otro, lo cual ocurría las más de las por impremeditadas duplicidades del legislador[125]. En otras palabras, dos preceptos abarcan con diferente amplitud un mismo comportamiento típico desde perspectivas desvalorativas distintas[126]. Este criterio debe siempre tenerse en cuenta para evitar absurdas impunidades o despropósitos punitivos que pueden derivarse de una mala coordinación de los marcos penales de algunos tipos penales de estructura parecida, cuando no idéntica[127].

Es necesario descartar desde el inicio cualquier posibilidad de aplicar la regla de consunción entre estos tipos penales. Como se ha señalado, para que exista una relación de consunción es indispensable que entre ambos tipos se observe una diferencia sustancial de desvalor. Esta regla opera cuando el tipo aplicable absorbe el desvalor del desplazado, lo que supone que el primero represente una mayor cantidad de injusto. Sin embargo, dado que estos tipos y sus respectivas penas presentan una estructura y gravedad muy similares,

---

[123] Jimenez de Asúa, op. cit., p 561.
[124] Van Welzeel, op. cit., pág 497-498.
[125] Matus Acuña, Jean Pierre, *El concurso aparente de leyes*, Ediciones Jurídicas de Santiago, Santiago de Chile, 1.ª ed., 2008, p. 263.
[126] Díez Ripollés, *Derecho Penal Español. Parte General en Esquemas*, 3.ª ed., Tirant lo Blanch, Valencia, 2011, pág 548.
[127] Muñoz Conde, op cit, p. 492.

resulta imposible afirmar la existencia de esa diferencia cualitativa. Por ello, la consunción queda excluida desde el principio.

Ahora bien, determinar cuál es el principio que resuelve el concurso aparente de leyes penales entre ambos tipos de fraude informático no es sencillo. La complejidad de esta tarea se deriva en que ambos tipos se diferencian distintas hipótesis, las cuales hay que analizar por separado.

La primera distinción relevante consiste en diferenciar las hipótesis cuyo objeto material son datos informáticos de aquellas cuyo objeto son los sistemas informáticos. En el capítulo anterior se estableció que una de las diferencias fundamentales entre ambos tipos de fraude informático radica precisamente en su objeto material. En efecto, la redacción del artículo 7° de la LDI permite concluir que todas las hipótesis allí previstas tienen como objeto material a los sistemas informáticos. Por su parte, el artículo 468° del Código penal contempla una hipótesis cuyo objeto material son datos informáticos y otra que, al igual que el tipo de fraude informático regulado en la LDI, tiene como objeto material un sistema informático.

Entre las hipótesis de fraude informático que tienen como objeto material sistemas y datos informáticos, no existe un concurso aparente de leyes penales. Esto se deriva de que en realidad, al tener un objeto material distinto, los tipos no sean aplicables a las mismas situaciones.

Manipular un sistema informático es distinto de manipular datos informáticos. En el primer caso, se interviene sobre el aparato electrónico en su conjunto, alterando su funcionamiento normal. Estos datos son solo el medio para lograr el objetivo, no el objeto directo de la conducta. En cambio, en la segunda situación, el delito se configura cuando la manipulación recae específicamente sobre datos informáticos contenidos en el sistema. Aquí, aquellos datos son el objeto de la acción, no un simple instrumento. Por lo tanto, ambos tipos se aplican a situaciones diferentes, lo que excluye la posibilidad de un concurso aparente de leyes penales.

En la otra vereda, el análisis de las hipótesis en que la manipulación recae sobre sistemas informáticos requiere nuevas distinciones. Esto se debe a que en la LDI se pueden identificar dos hipótesis. La primera, denominada estricta, tipifica la manipulación de sistemas informáticos vinculada a medios específicos de ejecución, como la introducción, alteración, daño o supresión de datos informáticos. La segunda, denominada amplia, contempla la manipulación mediante cualquier interferencia en el funcionamiento del sistema informático. A su vez, como se mencionó anteriormente, el artículo 468° del Código penal también prevé una hipótesis cuyo objeto material son los sistemas informáticos, aunque en este caso se exige afectar una función específica: la de procesamiento de datos.

Por lo tanto, el análisis del concurso aparente de leyes penales se debe hacer entre:

1. La manipulación del sistema informático se realiza mediante la introducción, alteración, daño o supresión de datos informáticos, sin afectar la función de procesamiento de datos del sistema.
2. La manipulación se realiza por medios distintos a la introducción, alteración, daño o supresión de datos informáticos sin afectar la función de procesamiento de datos.
3. La manipulación se realiza mediante la introducción, alteración, daño o supresión de datos informáticos y afecta la función de procesamiento de datos.
4. La manipulación se realiza por medios distintos a la introducción, alteración, daño o supresión de datos informáticos y afecta a la función de procesamiento de datos.

En la primera hipótesis, donde la manipulación del sistema informático se realiza mediante la introducción, alteración, daño o supresión de datos informáticos, sin afectar la función de procesamiento de datos, se debe aplicar el tipo del artículo 7° de la LDI. Lo anterior se fundamenta en que, si no se afecta la función de procesamiento de datos prevista en el artículo 468° del Código penal, no puede sostenerse que la conducta sea típica conforme al tipo penal establecido en dicho artículo.

En la segunda hipótesis, donde la manipulación se realiza por medios distintos a la introducción, alteración, daño o supresión de datos informáticos sin afectar la función de procesamiento de datos también se debe aplicar el tipo del artículo 7° de la LDI. El fundamento es el mismo que se acaba de entregar. Si no se afecta la función de procesamiento de datos prevista en el artículo 468° del Código penal, no puede sostenerse que la conducta sea típica conforme al tipo penal establecido en dicho artículo.

En la tercera hipótesis, donde la manipulación se realiza mediante la introducción, alteración, daño o supresión de datos informáticos y, además, se afecta la función de procesamiento de datos, el concurso debe resolverse aplicando el principio de alternatividad. Este principio resulta pertinente porque concurren elementos propios de ambos tipos: por un lado, la manipulación del sistema informático (común a ambos); por otro, la intervención sobre datos informáticos (característica exclusiva del artículo 7° de la LDI) y la afectación de la función de procesamiento de datos (propia del artículo 468° del Código penal). En consecuencia, se configura una relación en la que los tipos comparten una zona común, pero ninguno comprende totalmente al otro, lo que corresponde a la imagen clásica de dos círculos secantes.

En sus inicios, la solución propuesta por el principio de alternatividad, cuando los delitos contemplaban penas distintas, consistía en aplicar la pena más severa. En la

formulación original de Binding, esta conclusión podría parecer arbitraria, pues no ofrecía una justificación sobre por qué el acusado debía verse perjudicado por los errores del legislador. Sin embargo, en la actualidad, dicha solución resulta aceptable, en tanto es compatible con lo dispuesto en el artículo 75 del Código penal.

Por lo tanto, para determinar a favor de que tipo se resuelve el concurso aparente hay que tener en cuenta las penalidades.

En el tramo superior, correspondiente a un perjuicio mayor a 400 UTM, prevalece la aplicación del tipo del Código penal, ya que el delito de fraude informático contempla una pena más severa: presidio menor en su grado máximo a presidio mayor en su grado mínimo (cuando el perjuicio supera las 40.000 UTM), mientras que la LDI sanciona con presidio menor en su grado mínimo a medio.

Por el contrario, en el tramo inferior, esto es, un perjuicio de hasta 4 UTM, siempre rige la sanción del artículo 7°, inciso 1°, de la LDI, que castiga todo detrimento hasta dicha cifra con una pena de 61 a 540 días de privación de libertad y multa de 1 a 10 UTM. En cambio, el Código penal establece presidio menor en su grado mínimo y multa de 5 UTM.

Finalmente, en el tramo intermedio (perjuicio patrimonial entre 4 y menos de 400 UTM), las penas son las mismas. No obstante, la mayoría de la doctrina sostiene que el artículo 468° deroga al artículo 7° de la LDI, aplicando el principio de que la ley nueva prevalece sobre la ley antigua y por lo tanto debería prevalecer el fraude informático contemplado en el Código penal.

En la última hipótesis, cuando la manipulación se realiza por medios distintos a la introducción, alteración, daño o supresión de datos informáticos y afecta la función de procesamiento de datos, debe prevalecer la aplicación del tipo de fraude informático, conforme al principio de especialidad. Ello se justifica porque el artículo 468° del Código penal contempla lo mismo que la hipótesis general del artículo 7° de la LDI, pero añade un elemento adicional: la exigencia de que la manipulación afecte el procesamiento de datos informáticos. En consecuencia, el tipo del artículo 468° es especial respecto del previsto en la LDI, lo que determina su aplicación preferente.

4° Conclusiones preliminares

El artículo 468 del Código penal y el artículo 7° de la Ley 21.459 no se encuentran en (una relación de derogación tácita, ya que regulan conductas con objetos materiales distintos datos informáticos en el primero y sistemas informáticos en el segundo), lo que permite afirmar que ambos tipos penales coexisten en el ordenamiento jurídico.

La eventual colisión entre estas disposiciones no se resuelve mediante criterios de vigencia normativa, sino a través de reglas de concurso aparente de leyes penales, aplicables según las hipótesis concretas. En este sentido, no procede aplicar un régimen de concurso real ni ideal, pues ello vulneraría los principios de non bis in idem y proporcionalidad, además de carecer de justificación material al tutelar los mismos bienes jurídicos.

La solución adecuada se encuentra en el concurso aparente, que se determina mediante los principios de especialidad y alternatividad. Cuando la manipulación no afecta la función de procesamiento de datos, corresponde aplicar el artículo 7° de la LDI, por ser el único tipo que describe la conducta.

En cambio, cuando concurren elementos de ambos tipos (manipulación mediante datos y afectación del procesamiento), se aplica el principio de alternatividad, resolviendo el concurso en favor del tipo con pena más grave, conforme al artículo 75 del Código penal.

Por su parte, cuando la manipulación afecta la función de procesamiento de datos por medios distintos a los previstos en la LDI, debe aplicarse el artículo 468 del Código penal, conforme al principio de especialidad.

Finalmente, en los casos de alternatividad, la preferencia normativa depende del monto del perjuicio: prevalece el Código penal en perjuicios superiores a 400 UTM, la LDI en perjuicios inferiores a 4 UTM, y en el tramo intermedio la doctrina mayoritaria opta por el artículo 468, aplicando el principio de que la ley posterior prevalece sobre la anterior.

Conclusiones finales

El fraude informático se ha incorporado en la mayoría de las legislaciones como respuesta a las lagunas de punición generadas por la incapacidad de los tipos penales tradicionales para sancionar conductas que ocasionan perjuicio mediante medios informáticos. En el caso chileno, la primera tipificación expresa de este delito se produjo con la promulgación de la Ley N.º 21.459, la cual se inspiró casi completamente en el Convenio de Budapest.

En general, los tipos de fraude informático en el ordenamiento jurídico chileno tienen una estructura similar, ya que ambos tipifican la generación de perjuicio patrimonial a través de la manipulación informática. Sin embargo, entre ambos existen diferencias que provocan que estos tengan una aplicación diferenciada. La primera de ellas se manifiesta en el objeto material del delito. En cuanto al objeto material, el tipo de fraude informático de la LDI, se concluye que este es el "sistema informático". Se llega a esta conclusión, en cuanto a la redacción del tipo castiga al que *"manipule un sistema informático"*. La conducta típica, es decir, la manipulación, debe recaer sobre dichos sistemas. En cambio, en el fraude informático del Código penal la manipulación debe recaer en "los datos contenidos en un sistema informático" o en la capacidad de procesamiento de datos del sistema. La segunda diferencia se manifiesta en el ámbito de los medios de ejecución. En el artículo 7° de la LDI se tipifica un delito con los medios de ejecución vinculados. Estos se corresponden con la introducción, alteración, daño y supresión de datos informáticos. Además, en este mismo artículo se contempla una modalidad amplia, según la cual la manipulación se puede cometer mediante cualquier intervención que afecte al normal funcionamiento del sistema. Por su parte, el artículo 468 del Código penal no vincula ningún medio de ejecución, por lo cual la manipulación de datos y del procesamiento informático de estos se puede realizar de cualquier forma. En tercer lugar, se observa una sutil diferencia en los aspectos subjetivos del tipo. En la LDI se exige que el delito sea cometido con la finalidad de obtener un beneficio económico para sí mismo o para un tercero. Mientras que, el Código penal sólo establece que se debe perseguir la obtención de un beneficio, no especificando el carácter de éste.

En cuanto al bien jurídico, puede afirmarse que el fraude informático constituye un delito de carácter complejo, cuyo bien jurídico tutelado admite un análisis desde una doble perspectiva: como un delito informático o como una defraudación. Si analizamos esta modalidad de fraude como un delito informático, podemos concluir que este, eventualmente, tutela lo que se denomina "funcionalidad informática". Esta protección es eventual, en cuanto la lesión solo se produce cuando los delitos informáticos se producen en el contexto de un ataque a redes computacionales o mediante internet. Por último, si analizamos este delito como una defraudación, es evidente que este es un delito que tutela al patrimonio como un bien jurídico. Que el bien tutelado sea el patrimonio se hace

evidente cuando, en ambos tipos de fraude informático, se exige un perjuicio patrimonial estimable en dinero para su consumación. Por otro lado, se puede considerar que el fraude informático es una defraudación, porque es un delito que utiliza medios inmateriales para producir un perjuicio patrimonial.

El artículo 468 del Código penal y el artículo 7° de la Ley 21.459 no se encuentran en (una relación de derogación tácita, ya que regulan conductas con objetos materiales distintos datos informáticos en el primero y sistemas informáticos en el segundo), lo que permite afirmar que ambos tipos penales coexisten en el ordenamiento jurídico.

La solución más adecuada para armonizar la coexistencia de ambos tipos penales se encuentra en la aplicación de las reglas del concurso aparente, particularmente mediante los principios de especialidad y alternatividad. Así, cuando la manipulación no afecta la función de procesamiento de datos, corresponde aplicar el artículo 7° de la Ley N.º 21.459, por ser el único tipo que describe la conducta. En cambio, cuando concurren elementos de ambos tipos (esto es, manipulación mediante datos y afectación del procesamiento), debe aplicarse el principio de alternatividad, resolviendo el conflicto en favor del tipo con la pena más grave, conforme al artículo 75 del Código Penal. Por su parte, cuando la manipulación afecta la función de procesamiento de datos por medios distintos a los previstos en la LDI, se impone la aplicación del artículo 468 del Código Penal, en virtud del principio de especialidad. Finalmente, en los supuestos regidos por alternatividad, la preferencia normativa se determina según el monto del perjuicio: prevalece el Código Penal en perjuicios superiores a 400 UTM, la LDI en perjuicios inferiores a 4 UTM, y en el tramo intermedio la doctrina mayoritaria opta por el artículo 468, aplicando el criterio de que la ley posterior desplaza a la anterior.

Bibliografía

1. ALESSANDRI-SOMARRIVA, *Derecho civil. Parte preliminar y parte general* (Explicaciones basadas en las versiones de sus clases, redactadas, ampliadas y actualizadas por Antonio Vodanovic H.), 5.ª ed., Santiago, 1990, t. I.
2. Antón Oneca, *Derecho penal. Parte general*, 2.ª ed., Akal, Madrid, 1986.
3. Barja de Quiroga, *El principio non bis in idem*, Editorial Dykinson, Madrid, 2004.
4. Bascuñán A., "El principio de lex mitior ante el Tribunal Constitucional", *Revista de Estudios de la Justicia*, núm. 23, 2015.
5. Bascuñán A., "Sobre la distinción entre derogación expresa y derogación tácita", en *Anuario de filosofía jurídica y social*, núm. 18.
6. Bascur Retamal, Gonzalo y Letonja Cepeda, Thommas, *Delitos informáticos*, DER Ediciones, Santiago de Chile, 2025.
7. Becker Viollier, "La implementación del Convenio de Budapest en Chile: Un análisis a propósito del proyecto legislativo que modifica la Ley 19.223", *Revista de Derecho Universidad de Concepción*, N.º 248, 2020.
8. BOLETÍN N.º 12.192-25, "Informe de la Comisión de Seguridad Pública", 2019.
9. Castrillón Santana, Modesto Fdo., et al., *Fundamentos de informática y programación para ingeniería*, Paraninfo, Madrid, 2011.
10. Cerezo Mir, *Derecho penal. Parte general*, B de F, Buenos Aires, 2008.
11. Corcoy, "Delitos de peligro y protección de bienes jurídico-penales supraindividuales", Editorial B de F, 2024, p. 215.
12. Cury, *Derecho penal: parte general*, Ediciones Universidad Católica de Chile, Santiago de Chile, 8.ª ed., 2005.
13. Díez Ripollés, *Derecho Penal Español. Parte General en esquemas*, 3.ª ed., Tirant lo Blanch, Valencia, 2011.
14. Etcheberry, *Derecho penal: parte general*, Editorial Jurídica, Santiago, 3.ª ed., 1998, t. II.
15. Gascón, M., "Cuestiones sobre la derogación", *Cuadernos de Filosofía del Derecho*, núm. 15-16, vol. II, 1994.
16. González Lillo, D., "El delito de receptación: bien jurídico ofendido y problemas de imputación subjetiva a la luz del artículo 456 bis A del Código Penal chileno", *Pro Jure. Revista de Derecho*, PUCV, vol. 63, 2024.
17. GUTIÉRREZ, *Fraude informático y estafa*, Editorial Ministerio de Justicia, Madrid, 1991.
18. Guzmán Dalbora, *Colectánea criminal. Estampas de la parte especial del Derecho penal*, Editorial B de F, Buenos Aires.
19. Hernández, "La esperada consagración de un genuino delito de fraude informático en el Derecho penal chileno (art. 7.º de la Ley N.º 21.459)", en Scheechler (ed.),

Riveros (coord.), *Los delitos informáticos: aspectos político-criminales, penales y procesales en la Ley N.º 21.459*, DER Ediciones, Santiago de Chile, 2024, p. 214.
20. Historia de la Ley N.º 19.223.
21. Historia de la Ley N.º 19.233.
22. Historia de la Ley N.º 21.459.
23. Hormazábal, "Consecuencias político-criminales y dogmáticas del principio de exclusiva protección de bienes jurídicos", *Revista de Derecho*, vol. XIV, 2003.
24. Jescheck, Hans-Heinrich, *Derecho Penal. Parte General*, Comares, Berlín.
25. Jiménez de Asúa, *Tratado de Derecho Penal*, Editorial Losada S.A., Buenos Aires, 1950, t. II.
26. Kindhäuser, Urs y Zimmermann, Till, *Derecho penal. Parte general*, vol. I, Tirant lo Blanch, Valencia, 1.ª ed., 2024.
27. Klug, *Problemas de la filosofía y de la pragmática del derecho*, Fontamara, Coyoacán, 2002.
28. Klug, "Sobre el concepto de concurso de leyes", en *Problemas fundamentales de la filosofía y de la pragmática del derecho*, Alfa, Barcelona-Caracas, 1989.
29. Mata, "Delitos cometidos mediante sistemas informáticos (estafas, difusión de materiales pornográficos, ciberterrorismo)", *Cuadernos Penales José María Lidón*, Universidad de Deusto, N.º 4, 2007.
30. Matus Acuña, Jean Pierre, *El concurso aparente de leyes*, Ediciones Jurídicas de Santiago, Santiago de Chile, 1.ª ed., 2008.
31. Mattus Ramírez, *Manual de Derecho penal chileno: parte general*, Tirant lo Blanch, Santiago de Chile, 2.ª ed., 2021.
32. Mayer, *Delitos económicos de estafa y otras defraudaciones*, DER Ediciones, Santiago, 2018.
33. Mayer, Max Ernst, *Derecho penal. Parte general*, B de F, Buenos Aires, 2007.
34. Mayer, "El bien jurídico en los delitos informáticos", *Revista Chilena de Derecho*, vol. 44, N.º 1, 2017.
35. Mayer-Calderón, "El delito de fraude informático: concepto y delimitación", *Revista Chilena de Derecho y Tecnología*, vol. 9, N.º 1, 2020.
36. Mayer-Vera, "La nueva Ley de delitos informáticos", *Revista de Ciencias Penales*, sexta época, vol. XLVIII, N.º 3, 2022.
37. Mezger, *Derecho penal: parte general*, Editorial Bibliográfica Argentina S.R.L., Buenos Aires, 1958.
38. Muñoz Conde y García Arán, *Derecho Penal. Parte General*, Tirant lo Blanch, 11.ª ed., 2022.
39. Navarro, "El concepto de delito informático según la nueva legislación chilena (Ley N.º 21.459)", *Revista de Política Criminal*, vol. 18, N.º 36, diciembre 2023.
40. Novoa, E., *Curso de Derecho Penal chileno*, Tomo I, Editorial Jurídica de Chile, Santiago, 1960.

41. Novoa, E., *Curso de Derecho Penal chileno*, Tomo II, Editorial Jurídica de Chile, Santiago, 1960.
42. Oliver Calderón, G., "Retroactividad e irretroactividad de las leyes penales", Editorial Jurídica de Chile, Santiago de Chile, 2007.
43. Oliver Calderón, G., "Delitos contra la propiedad", en Rodríguez Collao, L. (coord.), *Derecho penal. Parte especial*, vol. II, Tirant lo Blanch, España, 2022.
44. Ossandón Widow, M., "El delito de receptación aduanera y la normativización del dolo", *Revista Ius et Praxis*, año 14, núm. 1, 2008.
45. Politoff, Sergio; Matus, Jean Pierre y Ramírez, María Cecilia, *Lecciones de Derecho Penal chileno. Parte general*, 2.ª ed. actualizada, Editorial Jurídica de Chile, Santiago de Chile, 2004.
46. Politoff-Matus-Ramírez, *Lecciones de derecho penal chileno. Parte especial*, Editorial Jurídica de Chile, Santiago, 2005.
47. Quintano Ripollés, A., *Tratado de la Parte Especial del Derecho Penal*, 2.ª ed., vol. II, Madrid, 1972.
48. RAE, *Diccionario de la lengua española*, s. v. «informática», tercera acepción.
49. RAE, *Diccionario de la lengua española*, s. v. «manipular», primera acepción.
50. RAE, *Diccionario de la lengua española*, s. v. «manipular», tercera acepción.
51. RAE, *Diccionario de la lengua española*, s. v. «mediante», primera acepción.
52. Rivacoba, *El delito de contrato simulado*, Akal, Madrid, 1992.
53. Roxin, *Derecho Penal. Parte General*, Thomson Reuters-Civitas, Navarra, 1.ª ed., t. I.
54. Roxin, *Derecho Penal. Parte General*, Thomson Reuters-Civitas, Navarra, 1.ª ed., t. II.
55. Silva Sánchez, *Derecho Penal. Parte General*, Civitas / Aranzadi, Cizur Menor (Navarra), 2025.
56. Squella Narducci, *Introducción al derecho*, 7.ª ed., Thomson Reuters, Santiago de Chile, 2022.
57. Tiedemann, "Criminalidad mediante computadoras", *Nuevo Foro Penal*, N.º 30, octubre-diciembre 1985.
58. Van Weezel, *Curso de derecho penal. Parte general*, Ediciones UC, Santiago, 1.ª ed., 2023.
59. Velasco, E., *Delitos tecnológicos: definición, investigación y prueba en el proceso penal*, Editorial Sepin, Madrid, 2016.
60. Vera Vega, Jaime y Mayer Lux, Laura, *Delitos informáticos y cibercriminalidad. Aspectos sustantivos y procesales*, B de F, Buenos Aires, 2024.
61. Wall, D., "The Internet as a conduit for criminal activity", en April, P. (ed.), *Information Technology and the Criminal Justice System*, Sage, Thousand Oaks, 2005.

62. Wessels, Beulke y Satzger, *Derecho penal. Parte general: el delito y su estructura*, Instituto Pacífico, Lima, 1.ª ed., 2018.
63. Zaffaroni, *Manual de derecho penal. Parte general*, Editorial Ediar, Buenos Aires, 2.ª ed., 2006.