REVISTA CHILENA
DE DERECHO Y TECNOLOGÍA

VOL. 13 (2024) • e72469 • DOI 10.5354/0719-2584.2024.72469
RECIBIDO: 30/10/2023 • APROBADO: 28/8/2024 • PUBLICADO: 31/12/2024

DOCTRINA

La regulación chilena del delito de fraude informático en el contexto de las transacciones electrónicas

The Chilean regulation of the crime of computer fraud in the context of electronic transactions

Gonzalo Bascur Retamal
Universidad Austral de Chile

RESUMEN Este texto ofrece una interpretación del delito de fraude informático previsto en el artículo 468 del Código Penal y en el artículo 7 de la Ley 21.459, contemplando las modificaciones introducidas por la Ley 21.595 y las cuestiones que se consideran más relevantes para su aplicación.

PALABRAS CLAVE Ciberdelitos, delitos informáticos, estafa informática.

ABSTRACT This text offers an interpretation of the crime of computer fraud provided for in Article 468 of the Criminal Code and Article 7 of Law 21.459, taking into consideration the amendments introduced by Law 21.595, addressing the issues that are considered most relevant for its application.

KEYWORDS Cybercrimes, computer crimes, computer fraud.

Introducción

La entrada en vigor del artículo 7 inciso primero de la Ley 21.459 (LDI) significó la primera tipificación explícita de un fraude informático en sentido estricto en nuestro ordenamiento.[1] Esto es la producción de un perjuicio patrimonial, a través de actos de manipulación no consentida sobre datos informáticos o sobre un sistema informático, sin interacción comunicativa entre víctima y autor (Cabrera y Contreras, 2024: 206 y 207; Mayer y Oliver, 2020: 179 y Pastor, 2020: 270), subsanando los problemas inter-

1. La Ley 21.459, que establece normas sobre delitos informáticos, deroga la Ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest, fue publicada el 20 de junio de 2022.

pretativos que exhibían los delitos contra el patrimonio tradicionales para la subsunción de esta clase de hechos,[2] los que, cabe recalcar, estadísticamente exhiben mayor relevancia práctica en el contexto de los delitos ejecutados por medios informáticos (Müller, 2022: 39; Mayer y Oliver, 2020: 152, 153 y 174 y Miró, 2013: 7-17).

La utilización de la denominación *fraude informático* y no *estafa informática* se debe a que la doctrina mayoritariamente ha descartado este hecho como variante de este delito.[3] Básicamente porque el método ejecutivo no consiste en engañar a otro mediante inducción para que disponga por error de su patrimonio (autolesión), sino más bien en ejecutar una transferencia u operación patrimonial electrónica no consentida y, por regla general, sin conocimiento del ofendido (Arocena y Balcarce, 2018: 183 y Hernández, 2024: 210, 211 y 214), alterando o manipulando indebidamente datos informáticos (Aboso, 2017: 318 y Jijena, 2008: 149 y 154),[4] en el sentido de modificar la programación de un ordenador (Agudo, Jaén y Perrino, 2019: 107). Tampoco se admite su calificación como hurto,[5] puesto que no se trata del enriquecimiento ilícito vía aprehensión física (ruptura de custodia) de una cosa *corporal* ajena (Miró, 2013: 11 y Jijena, 2008: 149 y 154), ni el menoscabo de la propiedad *stricto sensu* como bien jurídico (Mayer y Oliver, 2020: 170), en la medida que el objeto de referencia está dado por registros o representaciones contables de situaciones patrimoniales de naturaleza virtual, tales como dinero *giral*, *contable* o *electrónico* (Hernández, 2024: 209).

Luego, el aspecto medular de su fisionomía típica como defraudación radica en el medio empleado para menoscabar el patrimonio ajeno.[6] Esto es, la manipulación o alteración indebida de datos informáticos o sistemas informáticos.[7] Básicamente, la intromisión directa por medios informáticos en un patrimonio ajeno (Hernández, 2024: 215 y 216), característica que lo erige como un tipo delictivo de ofensividad mixta (o pluriofensivo), en el sentido de afectar tanto i) el patrimonio individual como ii)

2. Lo resaltan, Becker y Viollier (2020: 84) y Matus y Ramírez (2021: 633). Detalladamente respecto a las posibilidades de subsunción previas a esta regulación, Magliona y López (1999: 207-238), Hernández (2024: 208-213), Oxman (2013: 219-257), así como también Rosenblut (2008: 256 y ss.).

3. Enfáticos al respecto, Donoso y Reusser (2021: 134 y 135), Mayer y Oliver (2020: 162-164), Oxman (2013: 251-257), Pastor (2020: 270 y 271) y Tiedemann (2010: 442). Decididamente en contra, desde una perspectiva estrictamente dogmática, Balmaceda (2009: 362-369), sin perjuicio de constituir opinión minoritaria en nuestro medio, como indica Mayer (2018a: 67 y 68). Críticos respecto de esta última tesis, Matus y Ramírez (2021: 641).

4. Lo cual constituye una hipótesis diferente a una genuina estafa perpetrada a través de la interacción con la víctima mediante dispositivos telemáticos, como apuntan Mayer (2018a: 67) y Miró (2013: 6, 7, 11 y 12).

5. Detalladamente, Mayer y Oliver (2020: 165-167), sin dar mayor importancia a la naturaleza corporal del objeto de la acción, lo cual se refuerza en Mayer (2023: 48, 57 y 58). Asimismo, Oxman (2013: 240 y 241).

6. Por lo mismo, como explican Cabrera y Contreras (2024: 223), también puede apreciarse en estos casos una estructura *en triángulo*, donde el disponente (por ejemplo, un banco) sea una persona diferente a la víctima.

7. Véase Mayer y Oliver (2020: 172, 176, 177 y 179), como también la propuesta de regulación planteada por Magliona y López (1999: 257-261).

la funcionalidad informática en sus dimensiones de integridad o confidencialidad.[8]

Ahora bien, a pesar de la tipificación expresa del fraude informático realizada en el artículo 7 inciso primero LDI, la Ley 21.595 sobre Delitos Económicos (LDE), publicada el 17 de agosto de 2023, tipificó prácticamente la misma conducta en el artículo 468 núm. 1 y 2 del Código Penal (CP)[9] y, en cierta forma, autoconsciente sobre un posible conflicto entre las normas, estableció una regla concursal (cláusula de subsidiariedad expresa) para zanjar la eventual concurrencia entre ambas figuras en el inciso quinto de esta última disposición.

Por otra parte, la LDE derogó (artículo 58) gran parte de las conductas tipificadas en el artículo 7 de la Ley 20.009 (LTP),[10] incluyendo al hecho tipificado en su inciso segundo, figura que, a nuestro juicio, también permitía castigar esta clase de conductas.[11] Adicionalmente, este hito, nos parece, representa que dicho contenido de ilicitud (artículo 7 LTP) se encontraría actualmente recogido en gran parte bajo el núm. 3 y en el inciso tercero del artículo 468 CP, como se verá (BCN, 2023: 156, 157, 567 y 568 y Balmaceda, Cox y Piña, 2023: 121 y 122).

En lo que sigue, se realiza un análisis dogmático del contenido del fraude informático según la regulación —que consideramos duplicada— prevista en el artículo 7 inciso primero LDI y en el artículo 468 núm. 1 y 2 CP, con énfasis en los problemas interpretativos que se advierten como más relevantes para la *praxis*.

La protección penal en el marco del comercio electrónico

El derecho penal ha evolucionado para castigar los atentados patrimoniales ejecutados en el contexto de la expansión del comercio electrónico (Aboso, 2017: 302 y 303) y, en particular, para regular adecuadamente formas empíricas de aparición de manipulaciones computacionales dañinas para el patrimonio, en tanto las disposiciones patrimoniales progresivamente se han tecnificado y son desarrolladas a través del tratamiento electrónico de datos (Kindhäuser, 2002: 650). Esto ha dado forma a instrumentos de pago inmateriales, diversos al efectivo, que son gestionados en soportes digitales de

8. Por todos, véase Bascur y Peña (2022: 3-7). Derechamente en contra, dado que la penalidad es casi idéntica a la estafa, Cabrera y Contreras (2024: 207-209).

9. Similar, Balmaceda, Cox y Piña (2023: 121) y Cabrera y Contreras (2024: 228).

10. Ley 20.009, publicada el 1 de abril de 2005, originalmente fue denominada «limita la responsabilidad de los usuarios de tarjetas de crédito por operaciones realizadas con tarjetas extraviadas, hurtadas o robadas», y actualmente es rubricada «establece un régimen de limitación de responsabilidad para titulares o usuarios de tarjetas de pago y transacciones electrónicas en caso de extravío, hurto, robo o fraude», debido a la modificación introducida por la Ley 21.234, publicada el 20 de mayo de 2020. Sobre esta última reforma, véase Mayer y Vera (2021: 519 y ss.).

11. Al respecto, Bascur y Peña (2022: 21-24). Este tipo delictivo se mantuvo en vigor desde el 20 de mayo de 2020 hasta el 16 de agosto de 2023. Durante dicho período, favorables a esta consideración, Balmaceda (2021: 612-617) y Matus y Ramírez (2021: 642-643).

intercambio, incluso a través de un terminal de teléfono o un reloj tipo smartwatch, que son caracterizados por su sencillez, inmediatez y ausencia de retorno —o dificultad en la recuperación del importe—, lo que ha permitido progresivamente transitar desde el dinero de plástico hacia el dinero virtual (Abadías, 2023: 25-27, 35, 36 y 47).

En el derecho comparado, la tipología delictiva que deriva de este fenómeno (comercio electrónico) consiste básicamente en i) fraudes mediante manipulación informática (intromisiones ilícitas en sistemas informáticos) y ii) conductas ilícitas o abusivas dadas por el empleo de tarjetas de crédito, débito o similares (incluyendo sus respectivos datos e instrumentos de pago puramente digitales) en todo dispositivo encaminado a operacionalizar diferentes medios de pago (constituya un soporte físico o puramente informático).[12]

De esta forma, correlativamente a dicho panorama, el ordenamiento chileno contempla en el caso de i) fraudes informáticos los delitos tipificados en el artículo 7 inciso primero LDI y en el artículo 468 núm. 1 y 2 CP; mientras que en el contexto ii) del empleo ilícito de tarjetas de pago, las figuras previstas en el artículo 7 literales a) y b) LTP,[13] y en el artículo 468 núm. 3 e inciso tercero CP.

Ahora bien, dado que este último género delictivo se encuentra en general asociado a ciertas operaciones informáticas (tarjetas de pago), es necesario efectuar una breve reseña de su contenido como introducción al fraude informático propiamente tal.[14]

Las modernas tarjetas de pago o crédito permiten i) reconocer una relación preexistente entre el titular y la entidad emisora, ii) generalmente, contienen en su forma física, aunque también en las tarjetas virtuales, cierta información valiosa —identificación personal, firma o fecha de caducidad— y, además, propiedad definitoria y iii) sirven como medio de pago sustitutivo de la moneda en efectivo (Solari, 2021: 5-7). Esta función de medio de pago, similar a las monedas y billetes, pero con la particularidad de que se trata de un objeto emanado de entidades privadas y no de la autoridad (naturaleza híbrida), justificaría el tratamiento penal autónomo de los comportamientos relativos a su empleo ilícito (Mayer y Vera, 2022: 524 y 525), independizándolos del género de las falsedades documentales, los delitos contra la propiedad y los atentados contra el patrimonio individual. Por ello, se considera que el injusto asociado a la utilización ilegal de esta clase de tarjetas consiste en el menoscabo de un bien jurídico colectivo o supraindividual, materializado en la fiabilidad, funcionamiento o estabilidad de los medios de pago —además del crédito y retiro de dinero en efectivo—, en tanto propiedad integrante del concepto de *orden público económico* en sentido estricto.[15]

12. Por todos, Choclán (2002: 250 y 251); y Magliona y López (1999: 181-205).

13. Con posterioridad a la publicación de la LDE, la Ley 21.673, publicada el 30 de mayo de 2024, derogó el listado de literales del artículo 7 (incluyendo aquellos subsistentes luego de la entrada en vigor de la LDE, esto es, letras f) y h), respectivamente), estableciendo solamente dos: letras a) y b).

14. Destaca este parentesco, Fernández (2022: 116).

15. Mayer y Vera (2021: 528-531, 532, 547 y 554) lo postulan como bien jurídico colectivo de base en

De *lex lata*, el derecho chileno reconoce a estos instrumentos como herramientas para efectuar operaciones electrónicas económicas y establece el régimen de responsabilidad por su utilización indebida en la LTP. En este sentido, el artículo 1 inciso primero LTP emplea el término *tarjetas de pago* y las define como «tarjetas de crédito, tarjetas de débito, tarjetas de pago con provisión de fondos, o cualquier otro sistema similar»[16] para regular los «casos de extravío, hurto, robo o fraude» con relación al «respectivo giro de emisión u operación de dichos instrumentos». La amplitud de este concepto permite considerar, inicialmente, instrumentos de pago actuales como los de naturaleza *contacless*, *PayPal*, *wallets* digitales, *Bizum*, *wearables*, códigos QR, medios de pago biométricos, criptomonedas, etcétera (Gallego, 2023: 570), siempre que constituyan sistemas de pago similares.

Por otra parte, el artículo 1 inciso segundo LTP señala que igual tratamiento —casos de hurto, robo o fraude— se dará a los «fraudes en transacciones electrónicas» y las define como:

> Aquellas operaciones realizadas por medios electrónicos que originen cargos y abonos o giros de dinero en cuentas corrientes bancarias, cuentas de depósitos a la vista, cuentas de provisión de fondos, tarjetas de pago u otros sistemas similares, tales como instrucciones de cargo en cuentas propias para abonar cuentas de terceros, incluyendo pagos y cargos automáticos, transferencias electrónicas de fondos, avances en efectivo, giros de dinero en cajeros automáticos y demás operaciones electrónicas contempladas en el contrato de prestación de servicios financieros respectivo.

Esto comprende «las transacciones efectuadas mediante portales web u otras plataformas electrónicas, informáticas, telefónicas o cualquier otro sistema similar dispuesto por la empresa bancaria o el proveedor del servicio financiero correspondiente». El artículo 1 inciso tercero LTP dispone que tanto las tarjetas de pago como los sistemas de transacciones electrónicas podrán ser denominados alternativamente como *medios de pago*.

En este contexto normativo (medios de pago) existen cinco hechos tipificados como delito. Los dos primeros se establecen en los literales a) y b) del artículo 7 LTP.[17]

---

estas infracciones. Similar postura tienen Arocena y Balcarce (2018: 176), aunque lo relegan a un papel *mediato* o de *ratio legis* y Tiedemann (2010: 403). Hernández (2008: 32), además del patrimonio (36 y 37), señala al *tráfico comercial* o, inclusive, desliza la *fe pública* (36). En este último sentido, Mayer y Oliver (2020: 168 y 169) aluden a la *funcionalidad documental*, mientras que, respecto al fraude informático, al *patrimonio* y la *funcionalidad informática* (174-175). Matus y Ramírez (2021: 643) señalan como uno de los intereses protegidos, la *seguridad de los medios de pago*. Por su parte, Rojas (2017:384-385) identifica la *función* que cumplen dichos instrumentos en el tráfico económico (equivalentes funcionales del dinero).

16. Por su parte, Matus y Ramírez (2021: 287) aluden a instrumentos electrónicos de pago y crédito.

17. Este esquema legal obedece a dos hitos. El primero consistió en la entrada en vigor de la LDE, que derogó los literales a), b) c), d) e) y g) del artículo 7 LTP, en tanto modalidades comisivas del tipo «uso fraudulento de tarjetas de pago y transacciones electrónicas», así como también eliminó el tipo delictivo –independiente– previsto en su inciso segundo. Posteriormente, con la dictación de la Ley 21.673,

El artículo 7 literal a), consiste en i) usar maliciosamente a) una tarjeta de pago, b) clave o c) credenciales de seguridad o autenticación que hayan sido ii) *bloqueadas* con iii) la finalidad de a) realizar pagos, b) transacciones electrónicas, c) giros en cajeros automáticos o d) «cualquier otra operación que corresponda exclusivamente al titular o usuario de ellas». Se trata de casos donde el tarjetahabiente (usuario) ha dado aviso al agente emisor para evitar fraudes (artículos 2 y 3 LTP) y este último ha bloqueado el funcionamiento del medio de pago (un cajero, aplicaciones, plataforma digital, etcétera).[18]

La segunda conducta se tipifica en el artículo 7 literal b) y consiste en i) obtener maliciosamente para sí o para un tercero ii) la cancelación indebida de los cargos o la restitución indebida de fondos iii) sea a) proporcionando datos o antecedentes falsos en la declaración jurada a que se refiere el artículo 4, b) desconociendo falsamente una o más operaciones con medios de pago de su titularidad, c) simulando la existencia de operaciones no autorizadas, provocándolas intencionalmente d) o presentándolas ante el emisor como ocurridas por causas o en circunstancias distintas a las verdaderas. En definitiva, se trata del castigo de la obtención de un pago indebido, por el usuario o un tercero, de una tarjeta de pago a través de una simulación o de un engaño dirigido al emisor, de manera similar al denominado fraude de seguros (artículo 470 núm. 10 CP).[19] Ambos hechos se castigan con 541 días hasta cinco años de privación de libertad y multa correspondiente al triple del monto defraudado (artículo 7 inciso primero LTP).

Como se aprecia, se trata de hipótesis bastante acotadas que relegan los supuestos más importantes para su tratamiento en el CP, circunstancia que explicaría la derogación de los antiguos literales a), b), c), d) e) y g), como también del inciso segundo del artículo 7 LTP, y la tipificación de conductas de esta naturaleza en el artículo 468, tanto en su núm. 3 como en su inciso tercero. Por lo anterior, consideramos que estas últimas disposiciones habrían de subrogar el contenido de las normas derogadas.

El Código Penal contempla otras tres conductas relacionadas a esta clase de injusto: en el núm. 3 y en la primera y segunda oración del inciso tercero del artículo 468 CP.[20]

---

los literales f) y h) pasaron a estar regulados, con variaciones, en las nuevas letras a) y b). Luego, hasta donde alcanzamos a ver, el actual panorama deja sin regulación explícita la falsificación de tarjetas de pago (antiguo artículo 7 a) LTP), la intermediación ilegal de las tarjetas en sí mismas –no de sus datos operativos específicamente considerados– (previo artículo 7 literales b) y c) LTP), y la suplantación del titular para obtener la autorización requerida por el emisor para realizar transacciones (antiguo artículo 7 literal g) LTP).

18. Mayer y Vera (2021: 540) y Hernández (2008: 2) destacan que constituye una conducta que puede realizar el propio titular de la tarjeta.

19. Lo afirman, Mayer y Vera (2021: 541 y 542). Por su parte, Cabrera y Contreras (2024: 211, 219 y 220), parecieran apreciar un campo de superposición entre esta conducta y aquella tipificada en el artículo 468 numeral 3), como se verá.

20. Luego, hasta donde alcanzamos a ver, el actual panorama deja sin regulación explícita la *falsifica-*

Así, en primer lugar, el artículo 468 núm. 3 CP tipifica i) la producción de un perjuicio patrimonial mediante ii) el uso de carácter ii) no autorizado iii) de a) una tarjeta de pago ajena o b) de los datos codificados en una tarjeta de pago que la identifiquen y habiliten como medio de pago.[21]

El tipo es de resultado y consiste en ocasionar un perjuicio patrimonial por el uso no autorizado de una tarjeta de pago ajena o de sus datos operativos. Este supuesto permite castigar el simple uso de una clave ajena para la realización de una transacción electrónica —representativa de la producción de un perjuicio patrimonial—,[22] con total independencia de su forma de obtención dado que solo se exige ajenidad de los datos,[23] lo que puede consistir en una tarjeta original (sustraída o no) o falsificada (clonada). Ello puede verificarse de modo tradicional, empleando la tarjeta materialmente en un sistema de pago (un dispositivo o terminal),[24] o bien de forma electrónica o digital, especialmente tratándose de instrumentos de pago inmateriales, al introducir la información necesaria en un sistema informático, generalmente una operación realizada por internet (el artículo 1 inciso segundo LTP reconoce como transacción electrónica aquella realizada mediante plataformas informáticas).[25]

Tal como se aprecia, el injusto basal se construye subjetivamente por la contrariedad de la operación con la voluntad del titular de la tarjeta de pago.[26] El hecho se castiga con las penas establecidas para el tipo de estafa en el artículo 467 CP, vale decir, según el monto de lo defraudado.

En segundo lugar, el artículo 468 inciso tercero primera oración tipifica la acción de i) obtención de carácter ii) indebida de iii) los datos codificados en una tarjeta de pago que la identifiquen y habiliten como medio de pago.[27] Esta disposición castiga

---

ción de tarjetas de pago (antiguo artículo 7 a) LTP), la *intermediación ilegal* de las *tarjetas* en sí mismas –no de sus datos operativos específicamente considerados– (previo artículo 7 literales b) y c) LTP), y la *suplantación* del titular para obtener la autorización requerida por el emisor para realizar transacciones (antiguo artículo 7 literal g) LTP).

21. Este tipo delictivo recoge el injusto previamente tipificado en el artículo 7 literal b (uso de una tarjeta de pago sustraída o falsificada) y en el literal d (uso de los datos de una tarjeta de pago para favorecer operaciones de terceros no autorizadas por el titular).

22. De forma similar opinan Mayer y Vera (2021: 538). Dopico (2018: 233) ejemplifica cómo operaciones que no constituyen un perjuicio patrimonial a reducción del límite del crédito y operaciones de traspaso entre cuentas de la víctima de modo con intención de irritarla.

23. Como afirma Hernández (2023: 25), una tipificación de esta naturaleza contempla incluso los supuestos en que el autorizado ha entregado voluntariamente los datos de operación.

24. Dopico (2018: 233) y Pastor (2020: 273) diferencian si se trata de una transacción electrónica o la extracción de efectivo.

25. En el contexto español, Quintero (2011: 84) reconoce ambas posibilidades.

26. Críticos al respecto, Abadías (2023: 47) y Dopico (2018: 232 y 233).

27. En principio, esta conducta recogería el injusto del previo artículo 7 inciso segundo LTP consistente en la obtención ilícita de la información asociada a una tarjeta de pago desde un sistema informático,

toda forma ilícita (indebida) de obtener la información necesaria para operar una tarjeta de pago, sin necesidad de perjuicio patrimonial. Acorde al texto legal, los datos deben extraerse desde una tarjeta de pago (codificados en, generalmente, banda magnética o chip),[28] de modo que, si la información se ha obtenido a través de métodos informáticos desde un sistema informático —un acto de intromisión informática—, este tipo delictivo no es aplicable.[29] Esta consideración, nos parece, permite delimitar claramente esta conducta de otras acciones que recaen específicamente sobre datos informáticos asociados a una tarjeta de pago en el medio informático, vale decir, los tipos de acceso ilícito y espionaje informático (artículo 2 LDI) o sabotaje contra un sistema informático (artículo 1 LDI).[30] Por lo anterior, en concreto, se trataría de la regulación de la fenomenología propia de la *clonación* (duplicación de datos) (BCN, 2023: 157) y el *skimming* (replicado mediante un dispositivo instalado subrepticiamente en el terminal o dispositivo de operación de la tarjeta),[31] sin perjuicio de las ulteriores innovaciones en la materia.

Ahora bien, con relación a la posesión o detentación de la información, por ejemplo, en tarjetas falsificadas o clonadas, nos parece que la tenencia se halla comprendida por el verbo *obtención* —y posterior mantenimiento de la posesión—. Esto permite deslindar la conducta de los tipos de receptación de datos informáticos en su variante de almacenamiento de datos con un fin ilícito, dado por realizar transacciones no autorizadas por el usuario, siempre cuando provenga alguno de los delitos-base (artículo 6 LDI), o del tipo delictivo de abuso de los dispositivos bajo su modalidad de obtención —y consecuente detentación— de datos informáticos para la posterior ejecución de alguno de los delitos-fines (artículo 8 LDI) (Bascur y Peña, 2022: 27-33).

En tercer lugar, la segunda oración del inciso tercero del artículo 468 CP castiga i) la a) adquisición o b) puesta a disposición de otro a cualquier título de ii) los referidos datos de una tarjeta de pago. Tal como se aprecia, se sanciona el ciclo de intermediación ilegal de claves (BCN, 2023: 157), por regla general, las actividades de transacción

---

aunque bajo el previo contexto regulativo se explicaba con nitidez que podía tratarse de la extracción informática desde un sistema informático, cuestión que la traslación de la figura hacia el artículo 468 CP, nos parece, mutaría su alcance y sentido, como se verá.

28. Como destaca Gallego (2023: 570), los números y claves de tarjetas de crédito o débito se obtienen por medios más o menos sofisticados (utilización de *spyware*, *keyloggers*, actos de ingeniería social como el *phishing*, el *pharming*, fraudes en banca on-line; clonado de tarjetas, *skimming*) o por medios más elementales (persona que se apodera momentáneamente de la tarjeta, introduce los datos para comprar un producto o servicio en Internet, o los facilita telefónicamente, y restituye inmediatamente la tarjeta).

29. Similar, Queralt (2015: 504 y 505).

30. La fenomenología actual puede consultarse en Fernández (2022: 1136-1138).

31. Al respecto, véase Balmaceda, Cox y Piña (2023: 122) y Mayer y Vera (2021: 521). Esta circunstancia permite captar gran parte de los casos regulados bajo el derogado artículo 7 literal a) LTP (falsificación de una tarjeta de pago).

comercial de los datos que permiten operar una tarjeta de pago.[32] La norma alude a los datos de la oración anterior, de modo que las acciones también recaen sobre datos codificados y que han sido extraídos desde una tarjeta de pago, no desde un sistema informático. Por ende, según esta lectura, el tipo constituye el equivalente funcional de la receptación de datos informáticos en su variante de comercialización, transferencia o almacenamiento de datos provenientes algún delito-base con finalidad ilícita, es decir, suplantación de identidad digital (artículo 6 LDI).

La realización de más de un tipo delictivo por un mismo sujeto debe ser evaluada conforme a la teoría del concurso aparente de delitos, por ejemplo, entre la obtención indebida de la información y el posterior uso de una tarjeta clonada (consunción).

Cada uno de estos hechos (inciso tercero del artículo 468 CP) se castiga con 541 días a tres años de privación de libertad y multa de seis a diez unidades tributarias mensuales (UTM).

En resumen, los tipos delictivos más relevantes, según lo que aquí interesa, tratándose de medios de pago, consisten en i) la obtención ilegal de los datos para utilizar una tarjeta de pago (artículo 468 inciso tercero, primera oración CP); intermediación ilegal de tales datos (artículo 468 inciso tercero, segunda oración CP); y la utilización no autorizada de la tarjeta para efectuar una transacción electrónica, vale decir, suplantación (artículo 468 núm. 3 CP).

Los tipos delictivos de fraude informático

Tal como fue adelantado, el hecho consistente en un fraude informático se encuentra sancionado en dos disposiciones, el artículo 468 núm. 1 y 2 CP y el artículo 7 inciso primero LDI.

El delito tipificado en el artículo 468 núm. 1 y 2 CP

Como se adelantó, el artículo 468 núm. 1 y 2 CP fue incorporado por la LDE el 17 de agosto de 2023. La disposición señala:

> 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:
>
> 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 este.
>
> Utilizando sin la autorización del titular una o más claves confidenciales que habiliten el acceso u operación de un sistema informático.

32. Este tipo delictivo recogería el injusto de las modalidades previamente tipificadas en el artículo 7 LTP, en sus literales d) y e).

La figura constituye un tipo de resultado con método comisivo especificado, vale decir, cuya estructura requiere i) la producción de un perjuicio patrimonial (resultado típico: «irrogue un perjuicio patrimonial a otra persona») mediante la ejecución de alguna de ii) las dos conductas taxativamente determinadas por el legislador en los núm. 1 y 2 del artículo 468 CP.

El perjuicio patrimonial constituye el resultado típico y puede ser comprendido bajo la teoría dominante en nuestro medio, esto es, mediante la concepción jurídico-económica del patrimonio (Mayer y Oliver, 2020: 174), de forma que el resultado se identifica con la producción de una disminución del valor monetario del mismo (Cabrera y Contreras, 2024: 222 y 223), en este caso, representado por cualquier operación electrónica vinculada con el ánimo de lucro exigido por el tipo, tal como una transferencia de fondos, de una deuda, la cancelación de aquella o el reconocimiento de un crédito, etcétera (Balmaceda, 2009: 305-307 y Choclán, 2002: 251, 255 y 256).[33]

La primera modalidad de conducta se tipifica en el núm. 1 del artículo 468 CP y consiste en la manipulación de los datos o del procesamiento informático de estos en un sistema informático, ejecutada a través de una *intromisión indebida* en su operación.[34] O, dicho de otra forma, la intervención en un proceso de tratamiento de datos mediante las cual se pueda manipular el resultado de este (Kindhäuser, 2002: 655), ejecutada a través de un ataque directo sobre los datos (Cabrera y Contreras, 2024: 210).

Lo que caracteriza a esta variante y la diferencia de la modalidad del núm. 2 es que el perjuicio se ocasiona *distorsionando* la configuración de datos o de un sistema informático (Mayer y Vera, 2022: 299), mientras que este último presupone el funcionamiento *técnicamente correcto* del sistema por el uso de la verdadera contraseña del titular (Fernández, 2022: 1144).[35]

Que la acción típica (manipulación) deba ejecutarse a través de una intromisión

33. El perjuicio patrimonial debe ser causado de forma directa, esto es, sin la intermediación de la actuación posterior del autor, de la víctima o de un tercero. Véase, Cabrera y Contreras (2024: 223).

34. En el derecho comparado, se han clasificado las modalidades de ejecución de fraude informático conforme al momento en que el autor incide sobre el proceso ejecutado por el respectivo sistema informático: durante el i) ingreso de los datos *(input)*, tal como incorporar movimientos falsos, eliminar la entrada de operaciones reales o incorporar acreedores; ii) actos perpetrados durante el tratamiento o procesamiento de los datos ya ingresados, como la desfiguración de los datos procesados (redondear sumas de dinero), efectuar asignaciones irregulares de dinero o eliminación de saldos negativos y, finalmente, iii) injerencias durante el momento de emisión de los resultados exteriores del proceso *(output)*. Entre otros, véase Aboso (2017: 324 y 325), Balmaceda (2009: 109, 111 y 114), Choclán (2002: 252 y 253), Galán (2005: 39), Magliona y López (1999: 191-195), Mata (2003: 63), Miró (2013: 14) y Rovira (2002: 121). Por su parte, Galán (2005: 571 y 572) añade momentos previos al inicio del procesamiento y la fase iv) de retroalimentación, tratándose de sistemas interconectados (2005: 575 y 576). En nuestro medio, véase Balmaceda (2021: 613).

35. Para el debate comparado acerca de lo que debe entenderse por *corrección* en el funcionamiento del proceso de tratamiento de datos, véase Galán (2005: 578 y ss.).

indebida en la operación del sistema informático, significa que se debe alterar el normal funcionamiento de este, sea en el almacenamiento o en el tratamiento de los datos (un funcionamiento anómalo), provocando así resultados inadecuados o extraños a los que debiera arrojar (Aboso, 2017: 317-323). Con mayor detalle, se trata de una operación distinta a la tecnológicamente prevista,[36] vale decir, diferente al manejo normal del sistema (Dopico, 2018: 230), transgrediendo los medios técnicos de operación o desempeño de la plataforma informática de pago, de forma similar a la exigida por el tipo de acceso ilícito (artículo 2 inciso primero LDI), pero con relación a la manera de operar del sistema (Hernández, 2023: 11-14). De esta forma, el tipo exige lo que en la discusión comparada se ha denominado el criterio objetivo para la determinación de la incorrección del funcionamiento del sistema de tratamiento automatizado de datos (Galán, 2005: 112 y ss.): es decir, comparar el proceso efectivamente desarrollado con el desenvolvimiento de un programa libre de fallos.

En este contexto, las acciones alternativas para generar el perjuicio patrimonial en el marco de la intromisión indebida se distinguen según el objeto de la acción. La primera variante recae sobre datos informáticos a través de su manipulación, lo cual, a nuestro juicio, representa una injerencia sobre los datos en los términos del contenido de las acciones típicas de la figura de sabotaje sobre datos informáticos (artículo 4 LDI),[37] esto es: alteración, daño y supresión, en el sentido de modificación. Vale decir, ocasionar una variación del alcance o contenido inicial de los datos sin destruirlos (Gorjón, 2021: 104);[38] la eliminación o desaparición de algunos,[39] o toda otra forma

36. Respecto a este hito, en el contexto del acceso ilícito, véase Hernández (2023: 20).

37. De esta opinión, en el derecho comparado, véase Aboso (2017: 318 y 319), Choclán (2002: 266 y 267), Dopico (2018: 230 y 231) y Fernández (2007: 48 y 49). En nuestro medio, expresamente Rosenblut (2008: 256 y 257), con relación a la normativa previa, y bajo el panorama actual, al menos de forma implícita, Mayer y Oliver (2020: 158, 171, 173, 176 y 177), al reconocer la similitud en la estructura del tipo con actos de sabotaje.

38. Por su parte, Magliona y López (1999: 168) consideran la introducción de datos erróneos, su transformación y desfiguración, así como también suprimir datos correctos. Como ejemplos de esta modalidad, Cabrera y Contreras (2024: 213 y 214) señalan el aumento de haberes del autor en un sistema de pago de nóminas de pago a proveedores, de modo que el programa abulte las acreencias que se tienen en contra de los deudores; incorporar un acreedor inexistente a un sistema de contabilidad para crear un crédito falso a favor del autor o de un tercero; incorporar transacciones inexistentes a un sistema de contabilidad a fin de ocultar bienes faltantes en el inventario, o el diseño de un programa informático, dolosa e incorrectamente, como uno destinado a calcular la suma adeudada por el autor a sus proveedores, con el fin de que los honorarios de estos sean menores a los que corresponden. Lo sostienen en nuestro medio, Donoso y Reusser (2021: 126). Cabrera y Contreras (2024: 215) plantean el caso, discutido en el derecho alemán, de quien altera el código de barras de un producto más caro por otro más barato para pagarlo en una caja de pago automático.

39. Cabrera y Correa (2024: 217) ejemplifican con el caso en que el autor borra de un sistema informático contable determinados valores relevantes, buscando alterar el resultado automatizado, por ejemplo, de pago o cobro de acreencias.

de afectar la posibilidad de utilización regular de los datos informáticos (De la Mata, 2018: 747-749; Magliona y López, 1999: 168 y 169). La segunda alternativa de conducta consiste en la manipulación del resultado del procesamiento informático de los datos por el respectivo sistema. Vale decir, también en sentido análogo al tipo de sabotaje contra un sistema informático (artículo 1 LDI), lo cual implica una incidencia sobre el funcionamiento regular del sistema,[40] ocasionando un desempeño irregular en el tratamiento automatizado o con relación a sus resultados —esencialmente, la transacción electrónica que representa el perjuicio patrimonial—.[41] En ambos casos, el sistema opera con dicha alteración sin reconocer su invalidez y desarrolla el proceso de manera autónoma hasta la producción del perjuicio patrimonial (Aboso, 2017: 324 y 357-359).

La segunda modalidad de conducta se tipifica en el núm. 2 del artículo 468 CP y consiste en la irrogación de un perjuicio patrimonial sin existir manipulación informática, sino que tan solo por el uso sin la autorización del titular de una o más claves confidenciales que habiliten el acceso u operación del sistema informático (Aboso, 2017: 325 y 326). Como se aprecia, esta hipótesis no requiere una interferencia o distorsión en el funcionamiento del sistema informático, por cuanto el método ejecutivo descrito constituye una forma técnicamente correcta de operación del programa (Cabrera y Contreras, 2024: 210 y 211), lo que constituye simplemente un uso indebido o incorrecto, circunstancia que aproxima su fisionomía de injusto más bien a una sustracción (Pastor, 2020: 271 y 272) o a una deslealtad patrimonial (Galán, 2005: 139), y se ratifica por constituir una hipótesis distinta a la del núm. 1 del artículo 468 CP (Hernández, 2024: 225).

Aquí se consagra un criterio subjetivo para la fundamentación del injusto: la divergencia entre la forma en que el programa procesará los datos que se introduzcan y la voluntad de aquel que estaba autorizado a disponer de los activos patrimoniales (Galán, 2005: 112).[42] De ahí que la figura tipifique la suplantación del titular para la realización de una operación de transacción electrónica —uso de claves o datos ajenos—, con total independencia de la forma en que fue conseguida la respectiva contraseña (por ejemplo, si ha sido obtenida por engaño, coacción o si es que se encontraba ya alma-

40. Para Cabrera y Contreras (2024: 218), abarcaría la manipulación del *hardware* y de los registros físicos que se obtienen del procesamiento automatizado (la falsificación de los certificados emitidos por un sistema informático).

41. Como señalan Cabrera y Correa (2024: 218 y 219), se captarían hipótesis donde no se incide directamente sobre el sistema, como el aprovechamiento del conocimiento antijurídicamente obtenido de una falla de un sistema informático, excluyéndose los casos en que dicho conocimiento no ha sido adquirido de forma ilícita (se usa un error preexistente, sin manipulación de datos), tales como errores en sistemas de cobro, ofertas irrisorias en internet, en un cajero automático o en un tragamonedas.

42. Cabrera y Contreras (2024: 222) ejemplifican con el supuesto en que el autor excede la autorización del titular para extraer cierta suma de dinero o que utiliza una tarjeta obtenida antijurídicamente.

cenada por defecto en un dispositivo ajeno), sin perjuicio de la eventual punibilidad del acto de robo de identidad digital.

Ahora bien, la delimitación entre este supuesto y la conducta del artículo 468 núm. 3 CP radica, a nuestro juicio, en el objeto del comportamiento. De esta forma, aquí no se trata del empleo informático de los datos codificados en una tarjeta de pago para realizar una transacción electrónica o el retiro de dinero en efectivo, sino que del empleo, también digital, de las credenciales, contraseñas y demás información necesaria para operar cualquier plataforma informática de pago, por regla general pero no exclusiva, una cuenta bancaria.[43] Como se aprecia, la diferencia es sutil tratándose de medios de pago puramente electrónicos como la operación de cuentas en línea que permiten realizar transacciones electrónicas, dependiendo si el uso se materializa con la información exclusiva de una tarjeta de pago o por datos adicionales que permiten una transacción electrónica.

El tipo exige que la conducta se ejecute «para obtener un provecho para sí o para un tercero», vale decir, lo caracteriza como uno de intención trascendente en su variante de tipo de resultado cortado (Cabrera y Contreras, 2024: 225). Se anticipa, a través de un elemento subjetivo del tipo el efectivo enriquecimiento del autor correlativo a la disposición patrimonial, lo que constituye el tradicional ánimo de lucro del derecho penal nuclear.

El delito tipificado en el artículo 7 inciso primero LDI

El artículo 7 inciso primero LDI entró en vigor el 20 de junio de 2022 y dispone lo siguiente:

> 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.

Como se aprecia, la disposición tipifica la producción de un perjuicio patrimonial, en los términos ya indicados, mediante la conducta de manipulación de un sistema informático, la cual resulta ejemplificada explícitamente a partir de la mayoría de los supuestos de sabotaje informático,[44] vale decir, las acciones de alteración (artículos 1

43. En forma similar, véase Pastor (2020: 272). Así, como apunta Hernández (2008: 32), no siempre la información de una tarjeta de pago corresponde estrictamente a la de una cuenta bancaria.

44. En este sentido, véase Balmaceda (2009: 94 y 95), Mayer y Vera (2020: 229), Mayer y Oliver (2020: 153), y, con matices, Donoso y Reusser (2021: 103-105). Lo reconoce como una posición de la doctrina nacional, en el caso de la regulación previa, Rosenblut (2008: 259 y 260). Por su parte, Oxman (2013: 213) califica el hecho como atentado contra la integridad y confidencialidad, además del patrimonio de la

y 4 LDI), daño (artículos 1 y 4 LDI), supresión (artículos 1 y 4 LDI) e introducción de datos informáticos (artículo 4 LDI).[45]

A diferencia del artículo 468 CP, la descripción típica no contiene especificación de i) lo indebido del comportamiento ni de ii) la contrariedad a la voluntad del titular de la manipulación de los respectivos datos o del funcionamiento del sistema.[46] Sin embargo, consideramos que una interpretación sistemática del precepto (artículo 22 inciso segundo del Código Civil), especialmente considerando su paralelismo con el tipo de estafa, en cuanto la graduación de la pena y en abstracto, por consistir en una injerencia negativa sobre intereses patrimoniales ajenos (Mayer y Vera, 2022: 298 y 299), además de su *nomen iuris* (fraude), abonan la consideración implícita de la falta de autorización para la operación y el carácter irregular del comportamiento como elementos de su tipicidad objetiva. Como expresa Hernández (2024: 222, 223 y 231), los verbos dan cuenta de distorsiones funcionales en la operación del sistema informático —funcionamiento técnicamente incorrecto— y, con ello, de una desviación de la conducta ordinaria de quien tiene acceso a los datos, circunstancia que constituiría una restricción interpretativa para las acciones típicas (similar, Cabrera y Contreras, 2024: 212 y 214).

Esta figura también constituye un tipo de resultado con método comisivo especificado, al exigir que el perjuicio patrimonial sea causado a través de alguna de las conductas establecidas específicamente por el legislador.[47]

Al igual que bajo el artículo 468 núm. 1 CP, el comportamiento es definido como la manipulación de un sistema informático, cuyas notas generales son delineadas por la acción residual que agruparía el sentido de todas aquellas específicamente previstas: «cualquier interferencia en el funcionamiento de un sistema informático» (similar, Mayer y Oliver, 2020: 177 y 178). Por ello, consideramos que la expresión *interferir* recogería el sentido de constituir una influencia en el procesamiento electrónico o informático de datos, en los términos de obtenerse un resultado diferente al corres-

entidad bancaria y a la confianza depositada por el titular de la cuenta.

45. Solo quedan fuera del tipo las acciones de transmisión y deterioro de datos contenidas en el artículo 1 LDI.

46. Detalladamente, bajo el esquema legal previo a la vigencia de la LDE, véase Bascur y Peña (2022: 17-24).

47. Una opinión de mayor amplitud presenta Hernández (2024: 225 y 226), para quien resultaría típico el perjuicio patrimonial no producido directamente por la acción de manipulación informática, sino que también los casos de operación técnicamente correcta del sistema, pero precedida de un ingreso indebido o técnicamente incorrecto y los supuestos de operación normal del sistema, precedidos de accesos técnicamente correctos, pero que derivan de una manipulación informática previa, como las variantes de *phishing* o *pharming*, todos casos materialmente plausibles de injusto, pero que, a nuestro juicio, no exhiben las propiedades típicas requeridas por el legislador, como se verá. Por otra parte, Hernández (2024: 220 y 221) llama la atención sobre la redacción, en el sentido que la utilización del gerundio podría dar a entender que el perjuicio sería un hecho concomitante y, por ende, interpretarlo como una condición objetiva de punibilidad, tesis que finalmente descarta.

pondiente según la programación inalterada (Galán, 2005: 164 y 165). Vale decir, una operación distorsionada del sistema,[48] en idéntico sentido a la intromisión indebida constitutiva de manipulación de datos o sistema informático exigida por el artículo 468 núm. 1 CP, lo cual resulta nítido tratándose de las acciones de i) alteración, ii) daño y iii) supresión de datos, bajo el significado que revisten en el tipo de sabotaje informático (artículos 1 y 4 LDI). Los casos prototípicos debiesen ser aquellos de introducción de programas informáticos maliciosos (*malware*) que alteren el funcionamiento del sistema informático (Hernández, 2024: 225 y 227), pero también aquellos de incidencia directa sobre el *hardware*, con consecuencias para el tratamiento de los datos.

Sin embargo, la previsión de la conducta de iv) introducción de datos puede generar dudas respecto de si consagra una hipótesis de simple uso no autorizado de datos (suplantación digital de identidad), en los términos del artículo 468 núm. 2 CP,[49] o bien representa también un supuesto de interferencia (más) en el sentido antedicho;[50] esto es, de causación de un desempeño irregular en el tratamiento de los datos por el sistema, cuestión ampliamente debatida en el derecho comparado (Aboso, 2017: 348 y 349; Balmaceda, 2009: 281-284; Choclán, 2002: 253-255; Dopico, 2018: 230; Fernández, 2007: 236-242 y Pastor, 2020: 271 y 272).[51]

En nuestra opinión, tomando en cuenta la regulación vigente (Cabrera y Contreras, 2024: 210, 211, 219 y 220),[52] especialmente su delimitación con el supuesto previsto en el núm. 2 del artículo 468 CP, con la introducción de datos se tipifica un caso de influencia anómala en el tratamiento electrónico de la información en el sentido del artículo 468 núm. 1 CP, de manera equivalente a la irregularidad informática exigida por el tipo de acceso ilícito y espionaje informático, artículo 2 LDI (Hernández, 2023: 11-14 y 21-25). Por ende, se trataría de un supuesto de manipulación en sentido estricto. La simple operación normal del sistema no obedecería a la restricción sistemática de una incidencia técnicamente anómala en él, de modo que son atípicas las incidencias sobre datos que no impliquen manipulación indebida, así como de tales acciones precedidas de ingresos previos al sistema sin vulneraciones técnicas para ello, tal como se confirma con la tipificación expresa de usos abusivos o simplemente indebidos de datos en los numerales 2) y 3) del artículo 468 inciso segundo CP (Hernández, 2024: 224 y 225).[53]

48. Idea planteada por Mayer y Oliver (2020: 172 y 173), con crítica a la actual tipificación (2020: 178).

49. El simple acto de suplantación digital, lo consideran un acto de manipulación informática punible: Faraldo (2007: 41-43), Fernández (2022: 1145 y 1146), Galán (2005: 585) y Miró (2013: 16, 29 y 43).

50. Favorables a esta lectura restrictiva, en el derecho comparado, véase Aboso (2017: 318 y 319), Choclán (2002: 266 y 267), Dopico (2018: 230 y 231), Fernández (2007: 48 y 49). Implícitamente, Mayer y Oliver (2020: 158, 171, 173, 176 y 177).

51. Detalladamente en el contexto de la regulación alemana, véase Galán (2005: 128-152).

52. Otra opinión, bajo el estado previo de la normativa, en Bascur y Peña (2022: 20). Esto es debidamente resaltado por Hernández (2024: 224).

53. Cabrera y Contreras (2024: 220-222) añaden los tipos de los artículos 7 literal h) LTP y 468 N° 3 CP.

Se exige, como elemento subjetivo del tipo, que las referidas acciones sean ejecutadas con «la finalidad de obtener un beneficio económico para sí o para un tercero», circunstancia (subjetiva) que diferencia los actos de manipulación o perturbación de los tipos de espionaje (artículo 2 LDI) o sabotaje informático (artículos 1 y 4 LDI) (Mayer y Oliver, 2020: 176 y Galán, 2005: 727), ya que otorga al hecho el sentido de la motivación de obtener un futuro enriquecimiento, propio o ajeno, y no el simple objeto de dañar los intereses de la víctima,[54] lo que constituye así, en nuestra opinión, un equivalente funcional al ánimo de lucro requerido en las figuras tradicionales (Mayer, 2023: 54 y 55; Hernández, 2024: 219) y da forma a un delito de resultado cortado.[55]

¿Qué tipo delictivo aplicar a un caso de fraude informático?

Luego, si consideramos que el artículo 468 núm. 1 CP y el artículo 7 inciso primero LDI castigan la manipulación ilícita y no autorizada sobre datos o sobre un sistema informático para ocasionar un perjuicio patrimonial, desde el plano de la relación lógico-semántica ambos tipos se encontrarían en relación de identidad recíproca, en tanto se constata una redundancia total de las propiedades típicas tenidas en cuenta por el legislador, lo que da origen a un concurso aparente de delitos.[56] Como detalla Hernández (2024: 231 y 232), el artículo 7 inciso primero LDI se superpone por completo con el artículo 468 núm. 1 CP, no así con la modalidad de abuso del núm. 2 CP.[57]

Ahora bien, con plena consciencia de hallarse eventualmente duplicando el contenido del artículo 7 inciso primero LDI en el artículo 468 núm. 1 CP, en lo que aquí interesa,[58] el legislador introdujo en el inciso quinto del artículo 468 CP la siguiente regla concursal o cláusula de subsidiariedad expresa: «Lo dispuesto en los incisos segundo y tercero de este artículo será aplicable si el hecho no tuviere mayor pena conforme a otra ley». Por ende, el primer paso para zanjar una posible concurrencia entre los tipos consiste en identificar los supuestos en que dicha cláusula resulta operativa.[59]

Como se dijo, los casos de abuso o uso indebido de datos (suplantación de identidad digital) no estarían regulados por el artículo 7 inciso primero LDI, por lo que no se

54. Para Mayer y Oliver (2020: 178), esta circunstancia representa el injusto patrimonial, además de propiamente informático de la figura.

55. Así lo conceptualiza Galán (2005: 755 y 756) y, con menor detalle, Mayer y Oliver (2020: 172).

56. Fundamental en nuestro medio, véase Maldonado (2022: 28-31) y Mañalich (2016: 505 y ss.).

57. Para Cabrera y Contreras (2024: 227), al parecer, existiría un solo caso regulado en el artículo 7 inciso primero LDI, dados por la manipulación de *hardware* como forma de interferencia en el funcionamiento del sistema informático, opinión que no se comparte, en la medida que el artículo 468 numeral 1) segunda parte captaría, a nuestro juicio, tales supuestos.

58. La regla también se aplica a las conductas de obtención e intermediación ilegal de claves o tarjetas de pago del artículo 468 inciso tercero CP.

59. Para Hernández (2024: 231-233) se habría generado un desplazamiento completo de la sanción a favor del artículo 468 CP.

puede configurar un concurso con el artículo 468 núm. 2 CP. Ambas figuras se encontrarían en una relación lógico-semántica de estricta alternatividad, heterogeneidad o exclusión (Mañalich, 2016: 518 y 521).

Por el contrario, los supuestos conflictivos estarían dados por el artículo 468 núm. 1 CP y el artículo 7 inciso primero LDI, donde efectivamente se presentaría una superposición o duplicación de injusto entre las figuras.

En este contexto, teniendo en consideración que el artículo 7 inciso primero LDI gradúa la penalidad con arreglo al valor del perjuicio; recogiendo las magnitudes hasta ese momento previstas en el artículo 467 CP y anteriores a la reforma de la LDA (entre una UTM hasta montos superiores a 400 UTM); y que, con matices, el artículo 468 participa de igual métrica, es posible sostener las siguientes soluciones.

En el vértice superior, siempre prevalece la sanción por el fraude tipificado en el artículo 468 CP en el tramo de un monto superior a 400 UTM (Hernández, 2024: 232),[60] pues el inciso segundo (tres años y un día hasta diez años de privación de libertad, crimen) y el núm. 1 del artículo 467 CP (tres años y un día hasta cinco años de privación de libertad y multa de 21 UTM a 300 UTM), superan lo establecido para el inciso segundo del artículo 7 LDI (tres años y un día hasta cinco años de privación de libertad y multa de 21 a 30 UTM).

Por otra parte, en el vértice inferior, esto es un perjuicio de hasta 4 UTM, siempre prevalece la sanción del artículo 7 inciso primero núm. 3 LDI, en tanto castiga todo detrimento ocasionado hasta dicha cifra (desde 61 días hasta 540 días y multa de una a diez UTM), mientras que el artículo 468 CP queda restringido al mismo problema que la estafa-falta, entre 0,1 y 1 UTM. Se trata de un hecho atípico, al no encontrarse regulado por el artículo 494 núm. 19 CP (Mayer, 2016: 191-196), mientras que el segmento entre una UTM y hasta cuatro UTM, regulado en el artículo 467 núm. 4 CP, con pena inferior tratándose de la multa, desde 61 días hasta 540 días y multa de una a cinco UTM.

En el caso de los tramos de más de cuatro UTM y menos de 40 UTM y el segmento superior e inferior a 400 UTM, ambos tipos delictivos presentan idéntica sanción: 541 días hasta tres años de privación de libertad y multa de seis UTM a diez UTM (artículo 467 núm. 3 y artículo 7 núm. 2 LDI), y tres años y un día hasta cinco años de privación de libertad y multa de 11 a 15 UTM (artículo 467 núm. 2 CP y artículo 7 núm. 1 LDI). De esta forma, la regla concursal del inciso 5 del artículo 468 CP se torna enteramente inútil para resolver el concurso aparente.

Por ello, dado que se trata de una relación lógico-semántica de identidad o redundancia total (idéntico ámbito de aplicación) y es responsabilidad del legislador esta duplicación,[61] el concurso debería ser solucionado a través del parámetro cronológico

60. El artículo 467 CP distingue entre montos superiores a 400 UTM hasta 4000 UTM y cantidades superiores a esta última cifra (variante constitutiva de crimen).

61. Similar, Matus (2005: 481 y 482).

(un problema de sucesión de normas).[62] Esto es, dando preferencia a la sanción del hecho bajo la pena del artículo 468 núm. 1 CP.[63]

Otras cuestiones relevantes

¿Colaboración en un fraude informático (artículo 7 inciso segundo LDI) y fraude del artículo 468 núm. 1 CP?

El artículo 7 inciso segundo LDI castiga al que facilite los medios para que se cometa el fraude informático tipificado en el artículo 7 inciso 1 LDI, regla diseñada para captar la fenomenología de los denominados muleros o intermediarios electrónicos, esto es, supuestos de facilitación de cuentas bancarias para la recepción de los fondos ilícitamente obtenidos, sin exigir acreditar la convergencia subjetiva entre los involucrados en la operación (Bascur y Peña, 2022: 25).

Luego, toda vez que, como se dijo, existe una relación lógico-semántica de identidad entre los tipos del artículo 7 inciso primero LDI y 468 núm. 1 CP, siempre la realización de uno implica la realización del otro. Por lo mismo, consideramos que la figura tipificada en el artículo 7 inciso segundo LDI resulta aplicable a pesar de castigarse, finalmente, el hecho bajo la calificación jurídica establecida en el artículo 468 núm. 2 CP (Bascur y Peña, 2022: 21-24).

Lo anterior, bajo el entendimiento del concurso aparente de delitos como la concurrencia de la efectiva realización de dos o más delitos coincidentes en su contenido de significación delictiva,[64] esto es, al reconocimiento de realización múltiple de dos o más tipos delictivos y no de un problema de interpretación entre estos —y que, por ello, se excluirían entre sí—, situándose el problema en la aplicación de las respectivas normas de sanción,[65] pero no de la constatación de la infracción a las correlativas normas de conducta con relación al hecho que las funda.[66]

Tipicidad de las acciones constitutivas de robo de identidad digital

En vista de que tanto en el artículo 468 CP como en el artículo 7 inciso primero LDI el resultado de perjuicio patrimonial deriva de la ejecución de la acción de manipulación informática —y de abuso de datos en el último caso— (Aboso, 2017: 317, 324 y 325), nos parece que resulta imposible subsumir bajo estas figuras el conjunto de acciones

62. Expresamente en estas constelaciones, véase Maldonado (2022: 28-31).

63. Para Cabrera y Correa (2024: 227) se aplicaría cualquiera de las normas.

64. Detalladamente, Maldonado (2020: 494 y ss.), quien denomina esta concepción del concurso aparente como *tesis de la aplicabilidad*. En esta línea, entre otros, véase Mañalich (2016:505 y ss.), Matus (2002: 60) y Ossandón (2018: 969-973).

65. En contra de esta solución, Hernández (2024: 233).

66. Un razonamiento similar respecto del parricidio en Ossandón (2022: 118 y 119).

ejecutadas previamente para la obtención no consentida de la información del titular que resulta necesaria para ejecutar las operaciones electrónicas defraudatorias.[67] Es decir, de aquellas conductas informáticas que constituyen mecanismos anteriores o preparatorios de la acción típica (Hernández, 2024: 216-218). En este contexto, es posible identificar claramente dos fases de desarrollo (Fernández: 2007, 240-242): i) una etapa de obtención y almacenamiento de los datos necesarios para realizarlas, también denominada robo de identidad digital,[68] y ii) la ejecución de la operación patrimonial electrónica propiamente tal, fase que involucra tanto actos de manipulación informática como también de suplantación de la identidad del usuario.

Tradicionalmente, los actos de robo de identidad digital han sido categorizados bajo dos grupos de casos (Aboso, 2017: 326-332, 335 y 336; Matus y Ramírez, 2021: 640 y 641; Mayer, 2018b: 173-176; Mayer y Oliver, 2020: 156-160; Miró, 2013: 7-11; Oxman, 2013: 215-218 y Rosenblut, 2008: 254 y 255): conductas denominadas i) *phishing*, que consisten en la obtención de la información del perjudicado sea mediante a) engaño, persuasión o amenaza, a través de correos electrónicos, SMS, mensajes de aplicaciones, etcétera, (*phishing* clásico) como también por b) la instalación subrepticia de un *software* malicioso en su respectivo sistema informático (*phishing* técnico); y los denominados actos de ii) *pharming*, esto es, la implantación de accesos o sitios web falsificados que permiten engañar al usuario para que ingrese por error sus datos reales y así estos puedan ser conocidos y registrados indebidamente por el autor. Con arreglo a lo dicho, esto es, el necesario condicionamiento del resultado de perjuicio patrimonial por la ejecución de la acción típica prevista por el legislador (manipulación informática o uso indebido de claves), tanto el *phishing* como el *pharming* son atípicos como fraude informático del artículo 7 inciso primero LDI y del artículo 468 núm. 1 y 2 CP (véase otra opinión en Hernández, 2024: 225 y 226).[69]

Sin perjuicio de lo anterior, los actos de robo de identidad digital en su variante de *phishing* pueden ser castigados, en su modalidad de introducción de *software* malicioso,[70]

67. En esta orientación, Mayer (2018b: 173 y 174), Mayer y Oliver (2020: 152, 153 y 156), Rosenblut (2008: 258). Similar, Aboso (2017: 325-332). Constatan la dificultad, Becker y Viollier (2020: 86 y 87). En contra, admitiendo su tipicidad a este título, Miró (2013: 28-31).

68. Se trata de identificadores digitales que pueden ser atribuidos a una persona, Aboso (2017: 303).

69. Durante la vigencia del artículo 7 inciso segundo LTP, tales hechos resultaban castigados bajo dicho título; véase Bascur y Peña (2022: 21-24) y Matus y Ramírez (2021: 642 y 643). Para un análisis de su contenido, véase Mayer y Vera (2021: 542-544, 548 y 549). Básicamente, con dicha norma se incriminaban acciones que podrían constituir actos preparatorios de la conducta de manipulación informática y atípicos como tentativa del artículo 7 inciso primero LDI. Lo destacan, Mayer y Oliver (2020: 167 y 168) y Miró (2013: 17 y 18).

70. Como apunta Hernández (2023: 22-25), el *phishing clásico*, esto es, la obtención de una clave de acceso mediante *ingeniería social*, por regla general, un engaño (envío de SMS, correos, etcétera), no representa la vulneración de medidas tecnológicas de seguridad y, por ende, un injusto informático propiamente tal. El autor propone una solución novedosa para castigar a quien ingresa a un sistema con

como atentados informáticos mediante los tipos delictivos de acceso ilícito (artículo 2 inciso primero LDI) o espionaje informático (artículo 2 inciso segundo),[71] según la evidencia con la que se cuente para acreditar el elemento subjetivo de esta última figura. Respecto del *pharming*, a través de las figuras de sabotaje contra un sistema informático por alteración de datos (artículo 1 LDI) o de falsificación informática en su alternativa de la intención de que los datos adulterados «sean tomados como auténticos» (artículo 5 LDI).[72] En uno y otro caso, se debe considerar un concurso aparente de delitos entre las figuras que resulten aplicables, prefiriendo una sola de ellas.[73]

A modo de cierre, respecto de la fase de ejecución de la operación patrimonial, es importante destacar que la realización del fraude informático del artículo 7 inciso primero LDI y del artículo 468 núm. 1 y 2 CP no realizan al mismo tiempo el tipo de usurpación de nombre (artículo 214 CP), siempre que la identidad digital no sea equivalente al nombre real de una persona (Oxman, 2013: 236 y 237). Por otra parte, los actos de sabotaje informático coetáneos a la ejecución (alteración), deben considerarse actos copenados como resultado de aplicación de la consunción como parámetro de preferencia en el contexto de un concurso aparente de delitos.[74]

Diligencias investigativas

En lo que aquí interesa, tanto el tipo del artículo 7 inciso primero LDI como el artículo 468 núm. 1 y 2 CP conllevan la posibilidad de realizar diligencias especiales de investigación.

En el primer caso, el artículo 12 LDI en sus inciso primero y segundo contempla las técnicas de i) interceptación telefónica u otros medios de comunicación (artículos 222 a 225 del Código Procesal Penal, CPP) y ii) otros medios técnicos de investigación (artículo 226 CPP), bajo la exigencia de autorización judicial, y expresamente sobre investigaciones de criminalidad individual, sujeta a un estándar de solicitud y fundamentación superior a las reglas generales. En su inciso tercero, regula el denominado agente encubierto en línea. Por su parte, respecto del artículo 468 núm. 1 CP,[75] el artículo 8 inciso primero LTP, con exigencia de autorización judicial, limita las diligencias de

---

la clave original, pero habiéndola obtenido previamente mediante lo que denomina *phishing técnico*, esto es, previa manipulación informática, en la medida que considera dicho acto previo compatible con la exigencia típica del artículo 2 inciso primero LDI de existir vulneración de medidas tecnológicas, en circunstancias que del texto legal más bien se desprende que se trataría de una característica de la acción típica, simultánea a su ejecución.

71. En el contexto español, véase Miró (2013: 21).

72. Similar, véase Mayer y Oliver (2020: 153, 158, 160).

73. También proponen esta solución Mayer y Oliver (2020: 161, 162 y 173).

74. Destacan estas relaciones concursales Mayer y Oliver (2020: 153 y 173).

75. Se regulan sobre el artículo 468 inciso segundo y tercero CP.

los artículos 222 a 226 CPP a la investigación de estructuras delictivas organizativas (asociación ilícita o agrupación u organización de personas). Asimismo, bajo los mismos requisitos, el inciso segundo permite utilizar entregas vigiladas, agentes encubiertos e informantes, todo ello con arreglo a los artículos 23 y 25 de la Ley 20.000.[76]

Nos parece, según el caso, que una u otra alternativa de medidas intrusivas pueden emplearse si el hecho representa la realización de los artículos 7 inciso primero LDI o 468 núm. 2 CP, con independencia de la calificación jurídica que finalmente se otorgue en la formalización, requerimiento o acusación.[77]

Consideraciones conclusivas

En el marco de la criminalización de actos vinculados al comercio electrónico o a las transacciones informáticas, entre los hechos que consideramos más relevantes, el estatuto nacional actual distingue, respecto de las acciones concernientes a tarjetas de pago, i) la producción de un perjuicio patrimonial mediante uso no autorizado de una tarjeta de pago ajena o de los datos que la identifiquen y habiliten como medio de pago (artículo 468 núm. 3 CP); y ii) la obtención indebida de los datos codificados en una tarjeta de pago (artículo 468 inciso tercero, primera oración CP); mientras que con relación a fraudes informáticos propiamente tales, esto es, operaciones electrónicas diversas al empleo indebido de una tarjeta de pago, i) la producción de perjuicio patrimonial por manipulación indebida y no autorizada sobre datos o sistemas informáticos (artículo 468 núm. 1 y artículo 7 inciso primero LDI) y la ii) producción de una perjuicio patrimonial por el uso sin autorización de una o más claves confidenciales que habiliten el acceso u operación del sistema informático (artículo 468 núm. 2 CP)

En los casos de superposición completa y recíproca del contenido de los tipos delictivos previstos en el artículo 7 inciso primero LTP y 468 núm. 1 CP (relación lógico-semántica de identidad), se debe aplicar la regla de subsidiariedad expresa del artículo 468 inciso 5 CP (a saber, montos del artículo 467 núm. primero e inciso segundo CP, y artículo 7 núm. 3 LDI), salvo en los casos donde esta última resulta inaplicable (artículos 467 núm. 3 CP y 7 núm. 2 LDI), dándose preferencia a la regla del artículo 468 núm. 1 CP en virtud del parámetro cronológico (sucesión de normas). Esta relación concursal también despliega efectos con relación a la aplicabilidad de la figura tipificada en el artículo 7 inciso segundo LDI y las diligencias investigativas de los artículos 12 LDI y 468 inciso cuarto CP. Finalmente, los casos de robo de identidad digital deben ser castigados mediante los tipos de acceso ilícito, espionaje, sabotaje o falsificación informática, según corresponda.

76. Ley 20.000 que sustituye la Ley 19.366, que sanciona el tráfico ilícito de estupefacientes y sustancias sicotrópicas, publicada el 16 de febrero de 2005.

77. Véase otra opinión en Hernández (2024: 232 y 233), para quien, sin embargo, las diferencias prácticas serían mínimas.

Referencias

Abadías, Alfredo (2023). «La nueva regulación del delito de uso fraudulento de medios de pago distintos del efectivo al albur de la reforma de 22 de diciembre de 2022: Un análisis del art. 249.1 b) y 249.2 b) del CP». *Estudios de Deusto*, 71 (1): 15-82. DOI: 10.18543/ed.2788.

Agudo, Enrique, Manuel Jaén y Ángel Perrino (2019). *Derecho penal aplicado. Parte especial. Delitos contra el patrimonio y contra el orden socioeconómico*. Madrid: Dykinson.

Aboso, Gustavo (2017). *Derecho penal cibernético*. Buenos Aires: BdeF.

Arocena, Gustavo y Fabián Balcarce (2018). *Defraudaciones*. Buenos Aires: Hammurabi.

Balmaceda, Gustavo (2009). *El delito de estafa informática*. Santiago: Ediciones Jurídicas de Santiago.

—. (2021). *Manual de derecho penal. Parte especial. Tomo 2*. 4.ª ed. Santiago: Librotecnia.

Balmaceda, Matías, Francisco Cox y Juan Ignacio Piña (2023). *Nuevo estatuto de los delitos económicos en Chile*. Santiago: BCP Ediciones.

Bascur, Gonzalo y Rodrigo Peña (2022). «Los delitos informáticos en Chile: Tipos delictivos, sanciones y reglas procesales de la Ley 21.459, primera parte». *Revista de Estudios de la Justicia*, 37: 1-38. DOI: 10.5354/0718-4735.2022.67885.

BCN, Biblioteca del Congreso Nacional (2023). *Historia de la Ley 21.595. Ley de Delitos Económicos.* Santiago: Biblioteca del Congreso Nacional. Disponible en https://tipg.link/QuYx.

Becker, Sebastián y Pablo Viollier (2020). «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), 248: 75-112. DOI: 10.29393/RD248-13ICSB20013.

Cabrera, Jorge y Lautaro Contreras (2024). «Capítulo 7. El delito de fraude informático». En Samuel Malamud y Guillermo Chahuán (directores), *Delitos informáticos. Análisis dogmático y comentarios a la Ley 21.459* (pp. 205-231). Valencia: Tirant lo Blanch.

Choclán, José Antonio (2002). «Infracciones patrimoniales en los procesos de transferencia de dinero». En Oscar Morales (director), *Delincuencia informática. Problemas de responsabilidad* (pp. 243-280). Madrid: Consejo General del Poder Judicial.

De la Mata, Norberto (2018). «Tema 18. Delitos contra los sistemas de información». En Norberto de la Mata, Jacobo Dopico, Juan Antonio Lascuraín y Adán Nieto (autores), *Derecho penal económico y de la empresa* (pp. 727-759). Madrid: Dykinson.

Donoso, Lorena y Carlos Reusser (2021). *Protección de datos personales*. Santiago: Academia Judicial de Chile. Disponible en https://bit.ly/3FkeCVY.

Dopico, Jacobo (2018). «Estafas y otros fraudes en el ámbito empresarial». En Norberto de la Mata, Jacobo Dopico, Juan Antonio Lascuraín y Adán Nieto (autores), *Derecho penal económico y de la empresa* (pp. 169-235). Madrid: Dykinson.

Faraldo, Patricia (2007). «Los conceptos de manipulación informática y artificio semejante en el delito de estafa informática». *Eguzkilore*, 21: 33-57. Disponible en https://bit.ly/3ukbbbr.

Fernández, Javier (2007). «Respuesta penal frente a fraudes cometidos en Internet: estafa, estafa informática y los nudos de la red». *Revista de Derecho Penal y Criminología*, 19: 217-243.

—. (2022). «Clásicas y nuevas conductas fraudulentas ejecutadas en la red y su subsunción en los tipos de estafa y estafa informática contenidos en el Código penal». En Víctor Gómez, Carolina Bolea, José Gallego, Juan Hortal y Ujala Joshi (directores), *Un modelo integral de Derecho penal: libro homenaje a la profesora Mirentxu Corcoy Bidasolo* (pp. 1135-1149). Madrid: Boletín Oficial del Estado.

Galán, Alfonso (2005). *El fraude y la estafa mediante sistemas informáticos. Análisis del artículo 248.2 C.P.* Valencia: Tirant lo Blanch.

Gallego, José (2023). «Teoría general. Estafa y otras modalidades (arts. 248-249, 251 bis)». En Mirenxtu Corcoy (directora), *Manual de derecho penal. Parte Especial. Tomo 1.* (pp. 561-575). 3.ª ed. Valencia: Tirant lo Blanch.

Gorjón, María Concepción (2021). «Sabotaje informático a infraestructuras críticas: Análisis de la realidad criminal recogida en los artículos 264 y 264 bis del Código Penal. Especial referencia a su comisión con finalidad terrorista». *Revista de Derecho Penal y Criminología*, 23: 77-124. DOI: 10.5944/rdpc.25.2021.28405.

Hernández, Héctor (2008). «Uso indebido de tarjetas falsificadas o sustraídas y de sus claves». *Política Criminal*, 5: 1-38. Disponible en https://bit.ly/3EUhpUp.

—. (2023). «Lo "indebido" del acceso indebido a un sistema informático». *Doctrina y Jurisprudencia Penal*, 50: 3-25.

—. (2024). «La esperada consagración de un genuino delito de fraude informático en el derecho penal chileno (art. 7 de la Ley 21.459)». En Christian Scheechler (editor), *Los delitos informáticos. Aspectos político-criminales, penales y procesales en la Ley 21.459* (pp. 207-237). Santiago: DER.

Jijena, Renato (2008). «Delitos informáticos, internet y derecho». En Luis Rodríguez (coordinador), *Delito, pena y proceso. Libro homenaje a la memoria del profesor Tito Solari Peralta* (pp. 145-162). Santiago: Jurídica de Chile.

Kindhäuser, Urs (2002). «La estafa mediante computadoras en el Código Penal alemán (§ 263a STGB)». En Santiago Mir, Juan Luis Modolell, José Gallego y Carlos Bello (coordinadores), *Estudios de derecho penal económico*. Traducción de Héctor Hernández Basualto (pp. 649-674). Caracas: Livrosca.

Magliona, Claudio y Macarena López (1999). *Delincuencia y fraude informático*. Santiago: Jurídica de Chile.

Maldonado, Francisco (2020). «Sobre la naturaleza del concurso aparente de leyes penales». *Política Criminal*, 15 (30): 493-525. Disponible en https://bit.ly/3VNvius.

—. (2022). «Apuntes metodológicos sobre el concurso de delitos». *Revista de Ciencias Penales*, 1: 13-48. Disponible en https://tipg.link/R89N.

Mañalich, Juan Pablo (2016). «El concurso aparente como herramienta de cuantificación penológica de hechos punibles». En Claudia Cárdenas y Jorge Ferdman (coordinadores), *El derecho penal como teoría y como práctica. Libro en homenaje a Alfredo Etcheberry Orthusteguy* (pp. 501-547). Santiago: Legal Publishing.

Mata, Ricardo (2003). *Delincuencia informática y derecho penal.* Managua: Hispamer.

Matus, Jean Pierre (2002). «La teoría del concurso aparente de leyes penales y el "resurgimiento" de la ley en principio desplazada». *Revista de Derecho* (Universidad Católica del Norte), 9: 27-68. Disponible en https://tipg.link/SPHv. —. (2005). «Los criterios de distinción entre el concurso de leyes y las restantes figuras concursales en el Código Penal español de 1995». *Anuario de Derecho Penal y Ciencias Penales*, 2 (58): 463-494. Disponible en https://tipg.link/QuZi.

Matus, Jean Pierre y María Cecilia Ramírez (2021). *Manual de derecho penal chileno. Parte especial*. 4.ª ed. Valencia: Tirant lo Blanch.

Mayer, Laura (2016). «Las paradojas de la estafa-falta». *Política Criminal*, 11 (21): 173-201. Disponible en: https://tipg.link/QuZl.

—. (2018a). *Delitos económicos de estafa y otras defraudaciones*. Santiago: DER.

—. (2018b). «Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos». *Ius et Praxis*, 24 (1): 159-206. Disponible en https://bit.ly/3EXFnoT.

—. (2023). «Comentario a la SJG Concepción de 16 de mayo de 2016 (RIT 4775-2014)». *Doctrina y Jurisprudencia Penal*, 50: 45-58.

Mayer, Laura y Guillermo Oliver (2020). «El delito de fraude informático: Concepto y delimitación». *Revista Chilena de Derecho y Tecnología*, 9 (1): 151-184. DOI: 10.5354/0719-2584.2020.57149.

Mayer, Laura y Jaime Vera (2021). «La nueva regulación del delito de uso fraudulento de tarjetas de pago y transacciones electrónicas». *Revista de Ciencias Penales*, 2: 519-558. Disponible en https://tipg.link/R89g.

—. (2022). «La nueva ley de delitos informáticos». *Revista de Ciencias Penales*, 3: 267-366.

Miró, Fernando (2013). «La respuesta penal al ciberfraude: Especial atención a la responsabilidad de los muleros del *phishing*». *Revista Electrónica de Ciencia Penal y Criminología*, 15: 1-56. Disponible en https://bit.ly/3B2ZTMk.

Müller, Catalina (2022). *El fraude informático y la responsabilidad penal en la nueva Ley 21.459*. Santiago: Hammurabi.

Ossandón, Magdalena (2018). «El legislador y el principio *ne bis in idem*». *Política Criminal*, 13 (26): 952-1002. Disponible en https://tipg.link/QuZr.

—. (2022). «Delitos contra la vida». En Luis Rodríguez (director), *Derecho penal. Parte especial. Volumen 1* (pp. 24-194). Valencia: Tirant lo Blanch.

Oxman, Nicolás (2013). «Estafas informáticas a través de internet: Acerca de la imputación penal del *phishing* y el *pharming*». *Revista de Derecho* (Pontificia Universidad Católica de Valparaíso), 41: 211-262. Disponible en https://bit.ly/3iyosKU.

Pastor, Nuria (2020). «Tema 9. El delito de estafa». En Jesús-María Silva (director), *Lecciones de derecho penal económico y de la empresa. Parte general y especial* (pp. 247-282). Barcelona: Atelier.

Queralt, Joan (2015). *Derecho penal español. Parte especial*. 7.ª edición. Valencia: Tirant lo Blanch.

Quintero, Gonzalo (2011). «Capítulo 6. De las defraudaciones». En Gonzalo Quintero (director), *Comentarios al Código Penal español. Tomo 3*. 6.ª edición. (pp. 77-121). Navarra: Aranzadi.

Rojas, Luis Emilio (2017). «Modelos de regulación de los delitos de falsedad y de los delitos patrimoniales». *Política Criminal*, 12 (23): 380-408. DOI: 10.4067/S0718-33992017000100010.

Rosenblut, Verónica (2008). «Punibilidad y tratamiento jurisprudencial de las conductas de *phishing* y fraude informático». *Revista Jurídica del Ministerio Público*, 35: 254-266. Disponible en: https://bit.ly/3XPsnmL.

Rovira, Enrique (2002). *Delincuencia informática y fraudes informáticos*. Granada: Comares.

Solari, Mariana (2021). «Del dinero de plástico al dinero intangible: Interpretación penal de las tarjetas de pago con especial consideración de la Directiva (UE) 2019/713». *Revista Electrónica de Ciencia Penal y Criminología*, 23: 1-51. Disponible en https://tipg.link/QuZx.

Tiedemann, Klaus (2010). *Manual de derecho penal económico. Parte general y especial*. Traducción por Alfonso Galán Muñoz (pp. 439-450). Valencia: Tirant lo Blanch.

Sobre el autor

Gonzalo Bascur Retamal es abogado, licenciado en Ciencias Jurídicas por la Universidad de Talca, magíster en Derecho Penal por las Universidades de Talca y Pompeu Fabra y docente de la Universidad Austral de Chile, sede Puerto Montt. Su correo electrónico es gonzalo_bascur@hotmail.com. https://orcid.org/0000-0003-1149-1012

REVISTA CHILENA DE DERECHO Y TECNOLOGÍA

La *Revista Chilena de Derecho y Tecnología* es una publicación académica semestral del Centro de Estudios en Derecho, Tecnología y Sociedad de la Facultad de Derecho de la Universidad de Chile, que tiene por objeto difundir en la comunidad jurídica los elementos necesarios para analizar y comprender los alcances y efectos que el desarrollo tecnológico y cultural han producido en la sociedad, especialmente su impacto en la ciencia jurídica.

DIRECTOR
Daniel Álvarez Valenzuela
(dalvarez@derecho.uchile.cl)

SITIO WEB
rchdt.uchile.cl

CORREO ELECTRÓNICO
rchdt@derecho.uchile.cl

La edición de textos, el diseño editorial
y la conversión a formatos electrónicos de este artículo
estuvieron a cargo de Tipográfica
(www.tipografica.io).