REVISTA CHILENA
DE DERECHO Y TECNOLOGÍA

VOL. 9 NÚM. 1 (2020) • PÁGS. 151-184 • DOI 10.5354/0719-2584.2020.53447
RECIBIDO: 29/4/2020 • APROBADO: 16/6/2020 • PUBLICADO: 30/6/2020

DOCTRINA

# El delito de fraude informático: Concepto y delimitación

*The crime of cyber fraud: Definition and delimitation*

**Laura Mayer Lux y Guillermo Oliver Calderón**
*Pontificia Universidad Católica de Valparaíso, Chile*

**RESUMEN** El artículo analiza el delito de fraude informático, con énfasis en su concepto y delimitación. Para ello, comienza examinando brevemente su injusto en relación con los restantes delitos informáticos. Luego, aborda su sentido y alcance, así como su vínculo con otras figuras delictivas. Por último, plantea algunas sugerencias para su futura regulación legal expresa, teniendo en cuenta lo que establece el Convenio sobre Ciberdelincuencia del Consejo de Europa.

**PALABRAS CLAVE** Cibercrimen, espionaje informático, sabotaje informático, *phishing*, estafa.

**ABSTRACT** This article analyses the crime of cyber fraud, with an emphasis on its definition and delimitation. To do this, it begins by briefly examining its unlawful character in regards to other cybercrimes. Then, it addresses its meaning and scope, as well as its relationship with other crimes. Finally, it offers some suggestions for a future legal regulation of cyber fraud considering what is established in the Convention on Cybercrime of the Council of Europe.

**KEYWORDS** Cybercrime, cyber espionage, cyber sabotage, phishing, fraud.

## Planteamiento del problema

En los últimos años, el fraude informático ha concitado un creciente interés de parte de la doctrina penal.[1] Tal interés resulta esperable, pues, desde el punto de vista de su importancia práctica, dicho delito constituye el protagonista indiscutido de la cibercriminalidad (véase Gutiérrez Francés, 1991: 87; Miró Llinares, 2013: 3; Tiedemann, 2011: 287). Más aún, el estudio sistemático del cibercrimen surge, precisamente, debido a la comisión de fraudes informáticos asociados a transferencias electrónicas de fondos, hace aproximadamente tres décadas (Picotti, 2013: 35). Hasta la fecha, el fraude informático ha continuado siendo el centro de los ciberdelitos, básicamente por el impacto económico[2] y la frecuencia práctica que caracteriza a su ejecución,[3] la que a su turno se ha visto potenciada por el auge del comercio electrónico.[4]

Pues bien, a pesar del interés que suscita el fraude informático y su relevancia práctica, todavía no existe absoluta claridad respecto de qué implica con exactitud llevar a cabo un comportamiento constitutivo de dicho ilícito.

En principio, y según veremos, la idea de fraude informático evoca la producción de un perjuicio patrimonial mediante la manipulación o alteración de datos o programas de sistemas informáticos. Sin embargo, si se consideran las conductas que normalmente se califican de tales, podrá constatarse que el término fraude informático es entendido de forma bastante más amplia y que, en ese sentido, bajo dicha denominación suelen incluirse comportamientos muy diversos.[5] Desde este punto de

1. Cuestión que puede advertirse tanto en obras generales sobre el cibercrimen, que le dedican varias de sus páginas (así, por ejemplo, Gercke y Brunst, 2009; Gillespie, 2016), como en trabajos monográficos destinados a examinarlo pormenorizadamente (por ejemplo, Balmaceda Hoyos, 2009; Suárez Sánchez, 2009).

2. Los diversos comportamientos que pueden calificarse de fraudes informáticos producen perjuicios económicos que, examinados de forma aislada, integran la pequeña y mediana criminalidad (en esa línea, Tiedemann, 2011: 287; de forma más general, Kochheim, 2015: 11-12, con referencias ulteriores), pero que si se analizan globalmente pueden significar daños patrimoniales de consideración (Balmaceda Hoyos, 2009: 75; Masís Solís, 2016: 109, con referencias ulteriores). De ahí que se les califique, por un sector de la doctrina, como parte integrante de la delincuencia económica (por todos, Tiedemann, 2011: 287 y ss.).

3. Véase ya Kaiser (1996: 882); asimismo, Miró Llinares (2013: 3). En relación con la frecuencia práctica de dicho delito, se destaca que la ejecución exitosa de un fraude informático repercutiría en las probabilidades de repetición de esa clase de ilícito, «incluso en múltiples ocasiones» (Rovira del Canto, 2002: 78, con referencias ulteriores).

4. En ese sentido, Fernández Teruelo (2011: 35), Grabosky (2009: 83-84, 95). En efecto, si consideramos los delitos informáticos en sentido estricto de más común ocurrencia, el fraude informático es por lejos el que se ubica en primer lugar, seguido de casos de espionaje informático y de sabotaje informático, entre otros. Véase, con referencias a estadísticas alemanas y españolas, Mayer (2018: 176). Véase, asimismo, para algunas estadísticas anglosajonas, Norris, Brookes y Dowell (2019: 231).

5. En la misma línea, Balmaceda Hoyos (2009: 108-109, 114). Véase también Magliona y López (1999: 13, 190 y ss., con referencias ulteriores).

vista, los problemas de delimitación del fraude informático pueden sistematizarse de la siguiente manera:

En primer lugar, la noción de fraude informático a veces es vinculada con conductas que en realidad corresponden a etapas de ejecución imperfecta (delito tentado o frustrado) e incluso a actos preparatorios de un fraude propiamente tal. En particular, los comportamientos de *phishing* y *pharming*, que por lo general se ejecutan en el contexto de operaciones bancarias,[6] son un buen ejemplo de la laxitud con la que se emplea aquella expresión. En otras palabras, aunque esas conductas en rigor no se identifican con la provocación de un perjuicio patrimonial a través de la manipulación o alteración de datos de sistemas informáticos, por lo general se incluyen dentro de una noción amplia de fraude informático.

En segundo lugar, el concepto de fraude informático en ocasiones es relacionado con comportamientos que corresponden a otros delitos informáticos o a otros ciberdelitos. Así, por ejemplo, suele vincularse al fraude informático con el *hacking* (Hong, 1997), noción que a su turno se utiliza de forma poco precisa, casi como sinónimo de ciberdelito (Kochheim, 2015: 601). En cualquier caso, si por *hacking* entendemos el acceso indebido a datos o programas de sistemas informáticos,[7] podrá advertirse que para cometer un fraude informático resultará necesario acceder (en forma indebida) a los datos o programas referidos. Ello hace que ambas conductas se encuentren en una potencial relación concursal.

Al mismo tiempo, puede plantearse un nexo entre el fraude informático y el sabotaje informático, ya que el primero por lo general se asocia con la alteración de datos, mientras que el segundo con su destrucción. Tal relación se constata si se revisa la descripción que el Convenio sobre Ciberdelincuencia del Consejo de Europa (CCCE), del 23 de noviembre de 2001 (y del que Chile pasó a ser parte el 28 de agosto de 2017), prevé para lo que denomina «ataques a la integridad de los datos» (artículo 4 número 1) y «fraude informático» (artículo 8), ilícitos que comparten algunas conductas, entre las que destacan las consistentes en alterar o suprimir datos.

En tercer lugar, el delito de fraude informático tradicionalmente ha sido relacio-

6. A partir de ello, se ha vinculado a dichos comportamientos con la idea de fraude informático. Sin embargo, también es imaginable que se lleven a cabo conductas de *phishing* o *pharming* desprovistas de una connotación patrimonial, por ejemplo, para la ejecución de un espionaje informático; e incluso no (necesariamente) delictivas, como cuando se obtiene información para el envío de correos *spam* con fines publicitarios. Véase Oxman (2013: 215).

7. En ese sentido, por ejemplo, Escalona Vásquez (2004: 149). No obstante, debe hacerse presente que el acceso indebido a datos o programas de sistemas informáticos también puede relacionarse con el concepto de *espionaje informático* (Mayer, 2017: 238, con referencias ulteriores), o bien, de acceso *indebido*, *no autorizado* (Moscoso Escobar, 2014: 29, con referencias ulteriores) o *ilícito* (véase el artículo 2 del Convenio sobre Ciberdelincuencia del Consejo de Europa) a los datos o programas de que se trate.

nado con la estafa, al punto que en legislaciones como la alemana[8] o la española[9] se les regula sucesiva o conjuntamente, lo que ha contribuido a aclarar las diferencias entre ambos ilícitos. En ese sentido, si bien ambas figuras delictivas tienen varios elementos en común, partiendo por la exigencia de un perjuicio patrimonial ajeno, las distingue el medio necesario para provocarlo, que en un caso es la manipulación de datos y, en otro, el engaño.[10]

En fin, es posible plantear un vínculo entre el fraude informático y otros delitos de la Parte Especial, entre los que destaca en particular el delito de hurto. En efecto, a pesar de que un sector de la doctrina interpreta la conducta de este último ilícito en términos materiales, también es posible hacerlo en un sentido normativo y entender que, por ejemplo, podría verificarse cuando se comete una apropiación de dinero a través de sistemas informáticos. Ello obliga a plantear los elementos distintivos de uno y otro, así como un tratamiento penal coherente con su gravedad.

A la luz de los problemas indicados, el presente trabajo aborda el delito de fraude informático, con énfasis en su concepto y delimitación. Dicho estudio pretende arribar a una noción *estricta* de fraude informático, en oposición a otras aproximaciones más laxas a dicha expresión. Con tal finalidad, el texto parte examinando brevemente el injusto del fraude informático en relación con los demás delitos informáticos. Luego, analiza su sentido y alcance, así como su nexo con otros ilícitos. Por último, plantea algunas sugerencias para su futura regulación legal expresa. El estudio combina análisis doctrinal y legal, incluido lo dispuesto en el CCCE.

## Aproximación al injusto de los delitos informáticos

El conjunto de delitos informáticos en sentido estricto, esto es, de los comportamientos que afectan el software o soporte lógico de un sistema de tratamiento automatizado de la información (Jijena Leiva, 1993: 364; Moscoso Escobar, 2014: 13), está compuesto por tres ilícitos principales: el sabotaje informático, el espionaje informático y el fraude informático (Mayer, 2018: 160 y ss.). A pesar de que ellos pueden llevarse a cabo sin recurrir a internet, los que mayor relevancia práctica tienen son, precisamente, perpetrados en el ciberespacio (Miró Llinares, 2012: 49).

Desde el punto de vista de los bienes jurídicos subyacentes a tales ilícitos, es posible afirmar que los delitos informáticos afectan diversos intereses (Magliona, 2002:

8. En el StGB, la estafa aparece regulada en la § 263, mientras que el fraude informático (que literalmente se denomina «estafa informática») lo está en la § 263a.

9. El Código Penal español regula en un mismo artículo (artículo 248) al tipo penal de estafa y al fraude informático, disponiendo que quien realiza este último comportamiento se considera reo de estafa.

10. Para la relación entre el fraude informático y la estafa consagrados en la legislación alemana véase, por ejemplo, Kindhäuser (1999); en cambio, para el vínculo entre el fraude informático y la estafa regulados en la legislación española véase, entre otros, Suárez Sánchez (2009).

384), cuestión que depende de la clase de información con la cual se relacionen.[11] Así, por ejemplo, el sabotaje informático puede impactar negativamente en la propiedad si se destruyen o inutilizan datos que tienen un valor económico.[12] En cambio, el espionaje informático puede afectar la seguridad de la nación, o bien, la intimidad, si los archivos a los que se accede de forma indebida contienen informaciones secretas de carácter militar o imágenes íntimas de un particular, respectivamente.[13] Por su parte, el fraude informático —al menos en la tradición europea continental— tiene una evidente connotación patrimonial[14] y un particular medio comisivo: la manipulación o alteración de datos o programas de sistemas de tratamiento automatizado de la información.[15]

Cada vez que los delitos informáticos en sentido estricto son cometidos a través de internet, ellos tienen, además, un bien jurídico común, llamado *funcionalidad informática*, que puede definirse como «aquel 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» (Mayer, 2017: 255). Esas condiciones pueden resultar vulneradas en la interacción que se genera en el ciberespacio, de forma similar a lo que acontece en el tráfico vehicular.[16] En tal caso, ilícitos como el sabotaje informático, el espionaje informático y el fraude informático asumirán un carácter pluriofensivo,[17] ya que su ejecución lesionará tanto los intereses relacionados con los datos como la funcionalidad informática, en los términos indicados.

11. Lo que es distinto a sostener que el bien jurídico de tales ilícitos sea, derechamente, la información. Así, López (2002: 404-205). Con matices, Jijena Leiva (1992: 171, 179).

12. En ese sentido, por ejemplo, Romeo Casabona (1988: 175). Véase también De la Mata Barranco y Hernández Díaz (2010: 161).

13. Con énfasis en la tutela de la privacidad, Medina Schulz (2014: 81).

14. Al punto que se lo interpreta como una figura complementaria, aunque de naturaleza distinta (Kindhäuser, 1999: 285 y ss.) a la estafa.

15. Véase García García-Cervigón (2008: 293), Gercke (2009: 96), Hilgendorf y Valerius (2012: 148, 157), Huerta Miranda y Líbano Manzur (1996: 124-125), Rosenblut (2008: 255) y, con matices, Picotti (2013: 38, 45).

16. Esta analogía surge a partir de la caracterización de internet como una «autopista de la información» (Escalona Vásquez, 2004: 163; Quintero Olivares, 2001: 370, 373), en la que interactúan innumerables individuos (más en detalle, Mayer, 2017: 249).

17. A favor del carácter pluriofensivo de los delitos informáticos en sentido estricto, pero con matices respecto de los intereses afectados, Magliona (2002: 384), Magliona y López, (1999: 204-205). En contra del sentido pluriofensivo de tales ilícitos, Oxman (2013: 225 y ss.).

## Sentido y alcance del fraude informático, relación entre dicho delito y otros ilícitos de la Parte Especial

En una primera aproximación, la noción de fraude informático se vincula con la producción de un perjuicio patrimonial mediante la manipulación o alteración de datos o programas de sistemas informáticos.[18] Debe reconocerse, sin embargo, que dicha forma de definir al fraude informático corresponde a lo que podría denominarse un concepto estricto de éste, de lo que se sigue que existen otras formas más laxas de concebir ese comportamiento.

Desde un punto de vista amplio, en cambio, el fraude informático es entendido de diversas maneras. Por una parte, es usual que en el concepto de fraude informático se incluyan conductas que no necesariamente son la causa (directa) del perjuicio patrimonial de la víctima, sino que corresponden a mecanismos orientados a, por ejemplo, conseguir datos indispensables para generarlo. Por otra parte, cuando se deja en un segundo plano el medio comisivo (manipulación o alteración de datos) y se centra la mirada en la provocación de un daño a intereses patrimoniales ajenos a través de sistemas informáticos, es posible que el fraude informático se confunda con otros delitos de la Parte Especial, que afectan al mismo bien jurídico y pueden llevarse a cabo, como la gran mayoría de los comportamientos delictivos, mediante tales sistemas.

Según podrá advertirse, una adecuada delimitación del fraude informático plantea la conveniencia de abandonar una aproximación laxa a dicho concepto y, por el contrario, destinar esfuerzos a definirlo de manera estricta, sobre la base de tres elementos copulativos: la conducta, el resultado y el ánimo del agente. Pero, antes de emprender esa tarea, resulta necesario deslindar al fraude informático de otros comportamientos con los que tradicionalmente ha sido vinculado a nivel doctrinal y normativo.

### Fraude informático, *phishing* y *pharming*

El fraude informático suele relacionarse con el *phishing* y —en menor medida— con el *pharming*. En la práctica, este último se vincula con la ejecución de operaciones bancarias, cuya verificación en línea constituye un ámbito idóneo para manipular o alterar datos o programas de sistemas informáticos, a fin de perjudicar el patrimonio de terceros.

Conceptualmente, el *phishing* implica una obtención fraudulenta de datos de identidad personales de clientes de bancos y de sus cuentas bancarias o tarjetas de crédito

18. En esa línea, Gutiérrez Francés (1991: 112), Magliona y López (1999: 196, 203, 232), Romeo Casabona (1988: 47) y Rosenblut (2008: 255). En cambio, identifica al fraude informático con las manipulaciones o alteraciones de datos, exista o no una afectación del patrimonio, Jijena Leiva (2008: 148-149).

(Miró Llinares, 2012: 306), orientada a ejecutar transacciones electrónicas a favor del agente (Kochheim, 2015: 622) o de terceros. Desde un punto de vista terminológico, el *phishing* evoca la «pesca» de información o el intento de que las eventuales víctimas «muerdan el anzuelo» y proporcionen (consciente o inconscientemente) los datos que busca el hechor (Miró Llinares, 2013: 7). En tanto supone emplear información personal ajena, el *phishing* usualmente es vinculado con el concepto de hurto o robo de identidad (Brody, Mulig y Kimball, 2007) (también conocido como *identity theft*).[19] Éste, a su vez, resulta muy favorecido en un contexto como el ciberespacio, caracterizado por el anonimato de sus usuarios (Brunst, 2009), muchos de los cuales ocultan «su verdadera identidad mediante una gran variedad de técnicas» (Agustina, 2009: 17).

Como suele ocurrir en materia de conductas fraudulentas, el *phishing* ha ido cambiando en lo que respecta a la forma de llevarlo a cabo. En efecto, es posible constatar diversas maneras de ejecución de dicho comportamiento, que pueden relacionarse con dos fases de desarrollo.

El *phishing* supuso, en una primera etapa, el recurso a la denominada «ingeniería social» (Flores Mendoza, 2014: 303), o sea, la manipulación de una persona destinada a que entregue determinadas informaciones (Krombholz y otros, 2014: 114) (por lo general, confidenciales) al agente. En concreto, en esta fase inicial el *phishing* implicó normalmente[20] el envío de correos *spam* a un número indiscriminado de destinatarios (Flores Mendoza, 2014: 303), presuntamente provenientes de fuentes fiables (Rosenblut, 2008: 254; Herzog, 2009: 479 y ss.), en los que se les solicitaba proporcionar informaciones relativas a sus cuentas bancarias (o similares) (Kochheim, 2015: 622). En algunas ocasiones, tales requerimientos iban acompañados de advertencias —o derechamente de amenazas—, en el sentido de que no entregar los datos solicitados iría seguido de la cancelación o el bloqueo de la cuenta respectiva (Fernández Teruelo, 2011: 38). Las entidades bancarias o análogas, ante el descubrimiento de esta forma de fraude, adoptaron medidas informativas y preventivas, en orden a sugerir a sus clientes ignorar cualquier correo electrónico que requiera la entrega de información personal. Lo suyo han hecho los medios de comunicación, que cada cierto tiempo advierten sobre la existencia de esta clase de conductas defraudatorias.

Justamente, el descubrimiento de dicha forma de perpetrar el *phishing* obligó a introducir cambios en sus medios comisivos. Con ello comienza una segunda fase, caracterizada por el uso de software maliciosos que, para conseguir informaciones personales de potenciales víctimas, atacan en forma directa las operaciones que éstas realizan (Kochheim, 2015: 6 y 410; véase también San Juan, Vozmediano y Verga-

19. Para referencias sobre dicho concepto, véase *infra*.

20. Otras posibles formas de comisión del *phishing* pueden consultarse en Fernández Teruelo (2011: 38), entre las que se cuentan el envío de «encuestas falsas en nombre de organismos oficiales que tienen por objeto recoger datos personales de los usuarios que decidan participar en ellas».

ra, 2009: 177, con referencias ulteriores). Esta etapa en el desarrollo de la conducta permite superar los inconvenientes que implica la interacción con otro individuo, que puede rechazar o ignorar los requerimientos de envío de información. Por el contrario, el empleo de un *malware* permite prescindir del comportamiento ajeno resultante de las capacidades persuasivas del hechor —cuestión que vincula al *phishing* más con la estafa—, para pasar a centrarse en las capacidades técnicas (informáticas) del agente —hecho que sitúa al *phishing* más en el ámbito de la criminalidad informática en sentido estricto—. Con todo, debe reconocerse que en esta segunda fase de desarrollo el *phishing* está lejos de ser una «pesca» destinada a que sus potenciales víctimas «muerdan un anzuelo». En cambio, más bien corresponde a un «ataque» respecto de datos o programas contenidos en un sistema informático, perpetrado, como se dijo, a través del uso de un software malicioso.

En otro orden de cosas, es posible que el *phishing*, con independencia de su medio concreto de comisión, conlleve la realización de otra clase de comportamientos. Así, puede que el *phisher* obtenga en forma fraudulenta los datos de identidad personales de clientes de bancos y de sus cuentas bancarias o tarjetas de crédito, y los emplee para perpetrar él mismo una conducta perjudicial para el patrimonio de la víctima (por ejemplo, hacer transferencias bancarias desde su cuenta o cargos a su cuenta). Pero también es posible que se limite a conseguir fraudulentamente esos datos y luego los comercialice (Oxman, 2013: 215), a fin de que sean otros quienes perjudiquen el patrimonio de la potencial víctima. En fin, otra alternativa imaginable es que operen intermediarios (conocidos también como «mulas» o «muleros»), que facilitan —ya sea consciente o inconscientemente— sus cuentas bancarias para recibir el dinero obtenido en forma fraudulenta, que luego traspasan al autor del fraude (Fernández Teruelo, 2011: 39; Miró Llinares, 2013: 31 y ss.).

Pues bien, si el fraude informático supone la producción de un perjuicio patrimonial mediante la manipulación o alteración de datos o programas de sistemas informáticos, es evidente que el *phishing*, en su primera etapa de desarrollo, no tiene una vinculación directa con éste. En ese sentido, si el agente obtiene mediante fraude informaciones que los propios usuarios le proporcionan, y luego hace transferencias que los perjudican patrimonialmente, no ha habido en sentido estricto una manipulación o alteración de datos o programas. Si bien la existencia de un engaño previo podría hacer pensar que estamos ante una estafa, la falta de una disposición patrimonial (perjudicial determinada por error) llevada a cabo por el sujeto engañado impide sancionar al agente de acuerdo con ese delito.[21] En cambio, el castigo de dicho comportamiento a título de espionaje informático (o *hacking*), supuesto que exista un acceso indebido a los datos, sí podría plantearse.

21. Sobre la disposición patrimonial (perjudicial determinada por error) como requisito indispensable de la estafa, véase Hernández Basualto (2003: 168) y Kindhäuser (1999: 287).

Por su parte, si el fraude informático importa la provocación de un daño patrimonial a través de la manipulación o alteración de datos o programas de sistemas informáticos, el *phishing* que se identifica con el empleo de un *malware*, orientado a conseguir informaciones personales de otros individuos mediante el ataque directo de las operaciones que ellos ejecutan, no necesariamente corresponderá a un genuino caso de fraude informático. En efecto, el solo hecho de obtener esos datos de las eventuales víctimas no supone, *per se*, un perjuicio patrimonial para ellas, el que sólo se verificará cuando se hagan las transferencias, cargos, etcétera, que disminuyan el activo de su patrimonio. La calificación jurídica de tal obtención será la de un espionaje informático (o *hacking*) consumado, por lo que debe descartarse la tentativa de fraude informático, pues no ha habido principio de ejecución de un comportamiento consistente en manipular o alterar datos o programas para perjudicar patrimonialmente a la víctima.

Conceptualmente, el *pharming* supone la creación y operación de un sitio web falso, muy parecido o igual al de una entidad bancaria (Miró Llinares, 2012: 306) o de otra naturaleza (Kochheim, 2015: 621) (por ejemplo, un sitio web de subastas como eBay). Considerado como un mecanismo más sofisticado para cometer ciberfraudes (Flores Mendoza, 2014: 304), al menos si se le compara con el *phishing*, el *pharming* implica modificar los contenidos del DNS (mediante la configuración del protocolo TCP/IP o del archivo Imhost), a fin de que la potencial víctima, al digitar la dirección web de su banco en su navegador, ingrese al sitio web falso, en el que entregará información confidencial al hechor (o *pharmer*) (Miró Llinares, 2012: 306). Como podrá advertirse, el vínculo entre *phishing* y *pharming* es evidente, al punto que es muy común que ambos se presenten en conjunto[22] o que se sostenga que el segundo es una mera variante del primero (Fernández Teruelo, 2011: 38).

En el caso específico del *pharming*, es posible que el usuario ingrese el nombre de la entidad bancaria en un buscador (por ejemplo, Google) o la dirección web del banco en la barra de direcciones y sea redirigido a un sitio web fraudulento, que ha sido previamente creado por el *pharmer*. En el primer supuesto (ingreso del nombre de la entidad bancaria en un buscador), lo usual es que el sitio falso aparezca al comienzo de los resultados de búsqueda —que es donde por lo general se posicionan las páginas auténticas— y que esa misma circunstancia lleve a que la eventual víctima elija dicha página entre todos los resultados obtenidos. En el segundo supuesto, por su parte (ingreso de la dirección web del banco en la barra de direcciones), puede que aparezca directamente la página web fraudulenta, o bien, que se abra una ventana en el navegador del usuario con el sitio falso. El *pharming*, al igual que el *phishing*, ha

22. Por ejemplo, cuando se envía a la eventual víctima un correo *spam*, que contiene un enlace, y se la conduce tras ingresar a él a un sitio web que emula el del banco respectivo, desde el cual se obtiene la información que se pretende (Rosenblut, 2008: 254).

ido cambiando y sumando nuevas formas de comisión, como la instalación de un *malware* con la sola visita del sitio web fraudulento de que se trate, que posibilita la ejecución de operaciones maliciosas (por ejemplo, espionaje de datos) en contra de las potenciales víctimas (Kochheim, 2015: 410).

De nuevo, si el fraude informático supone la producción de un perjuicio patrimonial mediante la manipulación o alteración de datos o programas de sistemas informáticos, es claro que el *pharming,* que implica la mera creación y operación de un sitio web falso, no puede identificarse con el primero. Ahora bien, y a diferencia de lo que ocurre en el caso del *phishing*, la sola creación y operación del sitio web fraudulento implicará, por cierto, una manipulación o alteración de datos o programas, pero no (o no todavía) un perjuicio patrimonial para la eventual víctima. Para ello, sería necesario que el agente haga transferencias o cargos respecto de la cuenta bancaria o análoga del afectado, cuestión que importa algo más que la mera creación y operación de un sitio web falso.

La calificación jurídica de esta última conducta no es una cuestión sencilla. Una alternativa es entender que el *pharming* puro, que no va acompañado del *phishing*, constituye un acto preparatorio de un fraude informático propiamente tal. Esta opción, sin embargo, puede acarrear la impunidad de la conducta, si es que el ordenamiento jurídico de que se trate no contempla el castigo de actos preparatorios de delitos informáticos. Por su parte, de acuerdo con las figuras que prevé el CCCE, sería posible plantear una sanción a título de sabotaje informático (o «ataques a la integridad de los datos», del artículo 4), en tanto ha habido alteración de datos; o bien, de falsificación informática (del artículo 7), si es que se estima que ha habido alteración de datos que genere datos no auténticos. Ambas alternativas deben superar una dificultad, a saber, que se considere que la intención del agente era la mera destrucción de los datos (sabotaje informático) o que los datos fuesen empleados para efectos legales como auténticos (falsificación informática) y no que existió un ánimo de lucro ilegítimo (fraude informático).

## Fraude informático, espionaje informático (o *hacking)* y sabotaje informático

También es posible plantear nexos entre el fraude informático y otros ciberdelitos, en particular, el espionaje informático (o *hacking*) y el sabotaje informático.

En primer lugar, tal vínculo surge debido a que todos esos delitos inciden en «datos informáticos». Estos últimos se encuentran expresamente definidos en el artículo 1 letra b) del CCCE, como «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».

Pero, además, según se señaló, cuando la conducta de cualquiera de esos delitos se ejecuta en el ciberespacio, ellos tienen un bien jurídico común, denominado *fun-*

*cionalidad informática*, sin perjuicio de la afectación de otros intereses públicos o privados.

Igualmente, debido a que se trata de ilícitos que forman parte de la delincuencia informática, comparten los elementos criminológicos de ese ámbito de la criminalidad, entre los que destacan en especial las condiciones favorables que ofrece el ciberespacio para llevar a cabo comportamientos de manera transnacional (Miró Llinares, 2012: 152 y ss.), así como con efectos lesivos para una gran cantidad de potenciales víctimas (Sieber, 2014: 439).

Desde el punto de vista de la conducta incriminada, si se parte de la base de que el espionaje informático implica acceder a y conocer (de manera indebida) datos de sistemas informáticos, advertiremos que los delitos de fraude informático y sabotaje informático suponen que tenga lugar ese acceso y eventual conocimiento de datos. Así, tratándose del fraude informático, debe reconocerse que para manipular o alterar datos o programas de sistemas de tratamiento automatizado de la información, con el objeto de provocar un daño en intereses patrimoniales ajenos, ha de verificarse un acceso y eventual conocimiento (indebido) previo de dichos datos. Tal circunstancia genera que el espionaje informático asuma el carácter de «delito presupuesto» del fraude informático.[23]

En el caso del sabotaje informático, puede igualmente constatarse que para destruir o inutilizar datos de sistemas informáticos, ha de tener lugar un acceso y eventual conocimiento (indebido) previo de dichos datos. Por tanto, en tal hipótesis también es posible afirmar que el espionaje informático presenta el carácter de «delito presupuesto» del sabotaje informático.[24] Este último nexo entre el espionaje informático y el sabotaje informático tiene relevancia en relación con el fraude informático, pues, como veremos, a falta de una norma que expresamente sancione a este último delito en la Ley 19.223, del 7 de junio de 1993, puede recurrirse a la tipificación del sabotaje informático para evitar la impunidad del comportamiento.

De otro lado, si se analizan los vínculos concursales entre esos tres delitos (fraude, espionaje y sabotaje informático), es posible distinguir aquél que se verifica entre el espionaje informático y el sabotaje informático, por una parte, y aquél que se genera entre el espionaje informático y el fraude informático, por la otra. En primer término, si se tiene en cuenta la sistemática de la Ley 19.223, que sugiere la regulación de delitos de aplicación alternativa; así como las penas consagradas para el espionaje

23. Una situación como la descrita no es inusual en materia penal. Algo similar ocurre entre la mayoría de las lesiones corporales y el homicidio, toda vez que para matar en gran parte de los casos resulta necesario herir, golpear o maltratar antes a la víctima. Véase, solamente, Cury (2011: 670).

24. Sin embargo, atendido que el conocimiento de los datos para la perpetración del fraude informático o del sabotaje informático puede ser eventual, es posible que surja un nexo entre el fraude o el sabotaje informático y una forma de ejecución imperfecta (tentativa) del espionaje informático.

informático y el sabotaje informático, que no prevén una regla explícita de acumulación aritmética, cabría plantear la existencia, por lo menos en la mayoría de los casos,[25] de un concurso de leyes, que se soluciona a favor del sabotaje informático de acuerdo con el principio de absorción. En segundo término, si se asume que, a pesar de la inexistencia de un auténtico tipo penal de fraude informático en el derecho chileno, las conductas que pueden calificarse de tales son subsumibles en el tipo penal de sabotaje informático (en tanto importan modificación de datos),[26] cabría afirmar nuevamente un concurso de leyes, por lo menos en la mayoría de los casos,[27] entre el espionaje informático y el sabotaje informático, que se soluciona a favor del sabotaje informático de acuerdo con el principio de absorción.[28]

## Fraude informático y estafa

El vínculo entre el fraude informático y la estafa es bastante evidente, al punto que los ordenamientos jurídicos alemán y español los regulan de manera sucesiva o conjunta, respectivamente, pues parten de la base de que ambos afectan intereses patrimoniales ajenos, sólo que a través de distintos medios. Tal forma de asumir la regulación de esas dos figuras delictivas ha llevado a que en la doctrina comparada se hable de tipos penales «paralelos» (Eisele, 2013: 168, con referencias ulteriores; en el mismo sentido, De la Mata Barranco y Hernández Díaz, 2010: 181; Hilgendorf y Valerius, 2012: 149; Picotti, 2013: 42, 45); o que la legislación alemana aluda, de manera impropia, a estafa y estafa computacional para dar cuenta de la estafa en sentido estricto y del fraude informático, respectivamente.

Decimos que se trata de una referencia impropia, pues la estructura típica del fraude informático es diversa a la de la estafa (por ejemplo, Faraldo Cabana, 2007: 36-37), cuestión que a su vez obedece a las diferencias que es posible constatar en los requisitos típicos de uno y otro ilícito. Como es sabido, la estafa es un delito que exige un engaño, un error, una disposición patrimonial y un perjuicio patrimonial, elementos que deben hallarse vinculados entre sí por una relación de causalidad (Etcheberry, 2010: 392; Kindhäuser, 1999: 287).

El error, en tanto efecto de la conducta engañosa, es entendido por la doctrina

25. En esa línea, no puede descartarse la verificación de un concurso medial entre el espionaje informático y el sabotaje informático, con eventual afectación de diversos bienes jurídicos, como cuando el agente debe primero acceder a los datos y conocerlos, para así establecer cuáles serán objeto de una posterior destrucción o alteración.

26. Sobre la posibilidad de subsumir comportamientos constitutivos de fraude informático en el tipo del artículo 3 de la Ley 19.223, véase Hernández Basualto (2001: 18).

27. Véase la nota 25.

28. Con todo, si se afirma que el fraude informático puede subsumirse en el espionaje informático (ya que implica un acceso a los datos), no habría propiamente un concurso de leyes penales.

mayoritaria como un fenómeno sicológico (Hernández Basualto, 2003: 166), más precisamente, como una falsa representación de la realidad (Bullemore y Mackinnon, 2018: 92 y Garrido Montt, 2011: 337), de lo que se sigue que sólo una persona natural puede incurrir en él (Etcheberry, 2010: 396-397; Jijena Leiva, 2008: 149; Politoff, Matus y Ramírez, 2011: 433). En términos análogos, se afirma que «conceptualmente, las máquinas no pueden ser engañadas en el sentido del tipo penal de estafa» (Hernández Basualto, 2003: 167),[29] o bien, que no es posible sostener la existencia de un error si lo que la conducta fraudulenta logra es alterar el funcionamiento de un sistema informático (Hernández Basualto, 2010: 30).

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 (Hermosilla y Aldoney, 2002: 419), o sea, en las que lo afectado por la conducta es una computadora y no una persona. Por el contrario, las conductas fraudulentas ejecutadas «respecto de» o «contra» sistemas informáticos suelen corresponder a hipótesis de fraude informático, el que a su turno se identifica, como ya se dijo, con la producción de un perjuicio patrimonial mediante la manipulación o alteración de datos o programas de sistemas informáticos.

Dichas hipótesis deben distinguirse de los fraudes llevados a cabo «mediante» o «a través» de computadoras, que son perfectamente subsumibles en el delito de estafa. En el fondo, ellos no se diferencian en términos relevantes de lo que coloquialmente se denomina «estafa telefónica», que no es otra cosa que un fraude por engaño ejecutado a través de un teléfono, por lo general móvil. Pues bien, así como puede perpetrarse una estafa gracias a la comunicación que se entabla con la víctima mediante un teléfono, también es posible llevar a cabo una estafa gracias a la comunicación que se genera con ella a través de una computadora, por ejemplo, mediante el envío de mensajes fraudulentos a través de un sitio de venta o de subasta de productos en internet.

La doctrina minoritaria, representada en Chile por Balmaceda Hoyos, estima que no existen inconvenientes para subsumir conductas constitutivas de fraude informático en el tipo penal de estafa (Balmaceda Hoyos, 2009: 123, 127), por varias razones. En primer lugar, ya que él descarta que el error sea un elemento autónomo de dicho ilícito (Balmaceda Hoyos, 2009: 127),[30] lo que sugiere que éste no tiene el sentido ni la relevancia que le asigna la doctrina mayoritaria en relación con la estructura del

29. Con más énfasis, Hernández Basualto (2001: 17): «En nuestra tradición jurídica debe descartarse un posible "engaño" y consecuente "error" del sistema informático: el error es un fenómeno sicológico que sólo puede darse en personas naturales y no en máquinas, de suerte que el "engaño" al sistema no es sino una metáfora sin relevancia legal».

30. En España, un razonamiento similar puede verse, por ejemplo, en Gutiérrez Francés (1991: 290 y ss., 585), quien agrega que, en el evento de atribuírsele al error el carácter de elemento autónomo del delito de estafa, las posibilidades de subsumir casos de fraude informático en este último delito pasan por abandonar la concepción sicológica relativa a aquél.

delito de estafa. En segundo lugar, porque él considera que el engaño no requiere como receptor a una persona física, pues basta «con que el falseamiento intencional de la realidad que el engaño implica se exteriorice» (Balmaceda Hoyos, 2009: 123). En tercer lugar, debido a que él asume que quien efectúa la disposición patrimonial determinada por error en tales supuestos no es la máquina, sino que la persona natural que previamente la ha programado (Balmaceda Hoyos, 2009: 123, 127).

A nuestro juicio, la tesis minoritaria tiene el inconveniente de chocar con la forma en que el delito de estafa se encuentra tipificado en nuestro ordenamiento jurídico penal. En efecto, la regulación de ese ilícito parte de la base de que existe un sujeto que comete el fraude y otro sujeto que lo sufre, cuestión que se advierte nítidamente cuando se castiga «al que defraudare a otro». Además, se alude al perjuicio patrimonial resultante de esa conducta, por ejemplo, en los artículos 467 y 468 del Código Penal. En esa misma línea, la estafa, como se halla regulada en el Código Penal, implica un vínculo entre personas, principalmente «porque solo entre ellas es posible que concurra el necesario proceso comunicativo de atribución de relevancia y significado a determinados actos y hechos que describen sus normas» (Oxman, 2013: 251). Es tal proceso comunicativo el que justifica que la estafa sea calificada como un «delito de comunicación» (Mayer, 2014: 1.024-1.025, 1.031), en el que ha de verificarse una interacción comunicativa o, de forma más exacta, un intercambio de información típicamente relevante entre dos sujetos: el autor del engaño y el disponente del patrimonio que incurre en error.

A lo anterior puede agregarse que resultaría extraño que el delito informático de mayor importancia práctica no se encuentre regulado en la ley destinada a ese efecto (la Ley 19.223, que Tipifica Figuras Penales Relativas a la Informática) y, en cambio, pueda subsumirse en disposiciones del Código Penal que, en términos generales, han mantenido su redacción desde que fueron creadas en 1874. En esa línea, como también ha ocurrido en otros ordenamientos jurídicos, el surgimiento de la informática y de las conductas delictivas relacionadas con ella ha obligado a los Estados a adaptar su legislación a esta nueva realidad. Por razones obvias, dicho fenómeno no pudo haber sido considerado por los redactores de nuestro Código, que, por lo demás, para su texto original consideraron hipótesis de estafa sumamente casuísticas y no algo así como una figura general de fraude con la que pudiera castigarse cualquier forma de afectación de intereses patrimoniales ajenos.

En suma, el fraude informático es un fraude, pero no un fraude por engaño como lo es la estafa, cuestión que implica una disparidad en el medio de provocación del perjuicio patrimonial y que sugiere una aplicación alternativa, o sea, de uno u otro tipo penal.

## Fraude informático y hurto

La relación entre el fraude informático y el hurto puede resultar algo sorpresiva y es, en efecto, poco planteada a nivel doctrinal. En ese sentido, en materia de criminalidad informática, si es que se alude al hurto, por lo general no es para referir la apropiación de especies muebles ajenas sin la voluntad del dueño y con ánimo de lucro (artículo 432 del Código Penal), sino para dar cuenta de la usurpación de nombre (artículo 214 del Código Penal) o de la suplantación de identidad. En relación con este último comportamiento, es probable que el uso en lengua castellana de los conceptos «hurto de identidad» (Salvadori, 2010: 61) o «robo de identidad» (Flores Mendoza, 2014: 301) provenga de una traducción directa del término anglosajón *identity theft* (véase, entre otros, Anderson, Durbin y Salinger, 2008).

El vínculo que aquí quiere plantearse entre el fraude informático y el hurto considera a este último delito en el primer sentido indicado, o sea, como figura básica de los delitos de apropiación. Sobre ese supuesto, el nexo entre fraude informático y hurto puede postularse al menos desde dos perspectivas.

En primer lugar, si se considera la clasificación de los delitos contra intereses patrimoniales, que tiene en cuenta la naturaleza del ataque contra dicho bien jurídico y distingue entre delitos de apropiación, por un lado, y delitos de destrucción, por el otro, tanto el hurto como el fraude informático integrarían la primera de dichas categorías. En ese orden de ideas, la doctrina en general está de acuerdo en que el hurto y la estafa son delitos que implican un desplazamiento patrimonial de hecho de la cosa que es su objeto material (Bullemore y Mackinnon, 2018: 23-24; Etcheberry, 2010: 294 y ss.),[31] lo que los opone a ilícitos como los estragos o los daños, en los que existe un atentado contra la integridad de la cosa (Garrido Montt, 2011: 154, 407). Pues bien, aquello que se predica de la estafa es perfectamente aplicable al fraude informático, ya que este último no se centra en la destrucción de datos —como el sabotaje informático—, sino en una apropiación de ciertas cosas, como la que paradigmáticamente se produce cuando se manipula el sitio web de un banco para hacer transferencias electrónicas hacia otras cuentas, con el consiguiente perjuicio patrimonial del titular de la cuenta afectada. Por ende, tanto el hurto como el fraude informático son delitos de apropiación, pero cuyo rasgo distintivo es el medio con el que se verifica la apropiación de cosas (muebles) ajenas.

En segundo lugar, y vinculado con lo anterior, también es usual que se afirme que el hurto es un delito de apropiación por «medios materiales», en tanto que la estafa es un delito de apropiación por «medios inmateriales» (Bullemore y Mackinnon, 2018:

31. Con todo, debe reconocerse que el término *apropiación* en materia de estafa tiene un sentido diverso, más laxo y menos técnico que en el ámbito del hurto, cuestión que se relaciona tanto con la conducta típica como con el objeto material y las particularidades del bien jurídico tutelado en uno y otro caso.

23-24). En específico, se sostiene que en los delitos de apropiación por medios materiales se requiere el empleo de energía física para concretar la apropiación (Etcheberry, 2010: 294), mientras que en los delitos de apropiación por medios inmateriales lo que hay es el uso de mecanismos preferentemente intelectuales (Aguilar Aranela, 2008: 30), que suelen identificarse con el engaño o con el abuso de confianza (Garrido Montt, 2011: 154). Otra vez, aquello que se dice de la estafa es también aplicable al fraude informático, debido a que este último no gira en torno al despliegue de energía física, sino que implica el uso de mecanismos informáticos,[32] que corresponden a la manipulación o alteración de datos o programas de sistemas informáticos. Por ello, tanto el hurto como el fraude informático son delitos de apropiación, pero cuyo elemento diferenciador es el medio con el que tiene lugar la apropiación de cosas (muebles) ajenas.

Ahora bien, lo interesante del vínculo entre el hurto y el fraude informático radica en que el primero de dichos delitos puede asimismo interpretarse en un sentido, si se quiere, menos físico y más inmaterial, cuestión que a su turno puede generar dificultades a la hora de calificar jurídicamente un determinado comportamiento. En esa línea, si bien es posible entender que el comportamiento apropiatorio del hurto supone una aprehensión física o material de una cosa mueble ajena, un sector de la doctrina lo concibe, con razón, en términos más abstractos (Etcheberry, 2010: 297), como la ruptura de la custodia ajena (Mañalich, 2018: 172) y la constitución de una nueva custodia sobre la cosa, con ánimo de señor y dueño (Oliver, 2013: 70-71). Ello provoca que lo central para efectos de definir la conducta típica del delito de hurto no sea su aspecto físico o espacial, sino su dimensión de sentido (Bascuñán Rodríguez, 2004: 300).

A la luz de esta última aproximación a la conducta típica del hurto, cabe preguntarse si es posible afirmar la verificación de dicho delito cuando un sujeto manipula datos o programas, por ejemplo, del sitio web de un banco, y logra con ello traspasar dineros hacia una cuenta corriente distinta, por cierto, sin la voluntad del dueño de los fondos ni del banco respectivo. En un caso como el señalado es evidente que no hubo una aprehensión física de dineros, cuestión que sería necesaria si el comportamiento apropiatorio es concebido en términos físicos. No obstante, si éste es interpretado como la ruptura de la custodia que se tiene sobre los mismos y la constitución de una nueva custodia relativa a ellos, con ánimo de señor y dueño, podría sostenerse que sí tendría aplicación el delito de hurto, toda vez que habría habido una apropiación, en el sentido indicado, de cosas muebles ajenas sin la voluntad de su dueño (y con ánimo de lucro).

Refuerza lo anterior el hecho de que el legislador chileno, al tipificar el hurto, solo

32. De forma análoga, García García-Cervigón (2008: 292), quien alude a un desplazamiento «virtual», «inaprensible» de activos patrimoniales.

exige que el agente se apropie bienes muebles, pero no indica medios específicos a través de los cuales necesariamente ha de verificarse dicha conducta. En otras palabras, el hurto es un delito de medios indeterminados (Oliver, 2013: 69). Por tanto, también sería imaginable un hurto mediante manipulación o alteración de datos o programas de sistemas informáticos, cuestión que a su vez generaría un concurso de leyes con las normas que regulan el fraude informático —ya sea *de lege lata*, recurriendo a alguno de los tipos de la Ley 19.993, sobre sabotaje o espionaje informático; ya sea *de lege ferenda*—. Dicho concurso, en general, tendría que resolverse a favor del fraude informático, en virtud del principio de especialidad; salvo que entren en consideración otras variables, como la eventual penalidad más elevada del hurto, circunstancia que podría hacer aplicable a esta última figura.

## Fraude informático y uso fraudulento de tarjetas de pago y transacciones electrónicas

La Ley 21.234, del 29 de mayo de 2020, introdujo importantes modificaciones a la Ley 20.009, del 1 de abril de 2005, que actualmente 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. Como es sabido, la Ley 20.009 ya contemplaba, en su artículo 5, el delito de uso indebido de tarjetas falsificadas o sustraídas y de sus claves (Hernández Basualto, 2008b), ilícito que fue trasladado al artículo 7 de la misma ley, así como ampliado de manera considerable en relación con su objeto material y con las conductas en él sancionadas.

En lo que aquí interesa, el artículo 7, en su inciso segundo, consagró un supuesto de uso fraudulento de tarjetas de pago y transacciones electrónicas, que castiga

> al que mediante cualquier engaño o simulación obtenga o vulnere la información y medidas de seguridad de una cuenta corriente bancaria, de una cuenta de depósito a la vista, de una cuenta de provisión de fondos, de una tarjeta de pago o de cualquier otro sistema similar, para fines de suplantar al titular o usuario y efectuar pagos o transacciones electrónicas.

En una primera aproximación, el tipo penal transcrito se relaciona con el fraude informático en virtud de uno de los contextos comisivos que suele caracterizar a este último comportamiento delictivo. En efecto, según ya se destacó, el estudio sistemático del cibercrimen nace debido a la perpetración de fraudes informáticos vinculados con transferencias electrónicas de fondos, circunstancia que prevé expresamente la hipótesis de uso fraudulento de tarjetas de pago y transacciones electrónicas, que analizamos.

Por otra parte, este último tipo penal forma parte del conjunto de delitos que requieren del empleo de tecnologías para ser ejecutados. Dicha noción es más amplia

que la de delito informático (en sentido estricto), pues no necesariamente implica que la conducta incida sobre datos o sistemas informáticos, como es propio de la criminalidad informática *stricto sensu*. Eso en parte justifica que los delitos relacionados con tarjetas de pago o similares se regulen fuera de la Ley 19.223, destinada a tipificar la criminalidad informática.

En la misma línea, la descripción del supuesto de uso fraudulento de tarjetas de pago y transacciones electrónicas, referido, contiene un elemento que lo aleja del fraude informático en sentido estricto y lo acerca a otra clase de conductas, como el *phishing* y la estafa. Se trata de la exigencia de engaño o simulación, términos que semánticamente significan lo mismo, y que suponen una interacción comunicativa entre personas: una que emite un mensaje relativo a determinados hechos y otra que recibe e interpreta la información en él contenida.[33] Por el contrario, el comportamiento característico del fraude informático es la manipulación de datos de sistemas informáticos, para la cual no resulta necesaria interacción comunicativa alguna entre dos individuos.

Lo anterior no se ve alterado por el hecho de que el tipo del inciso segundo del artículo 7 de la Ley 20.009 aluda en forma expresa a pagos o transacciones electrónicas, ya que es perfectamente posible que se ejecute un comportamiento delictivo, en relación con ellos, sin que se lleve a cabo un fraude informático en los términos indicados. Más todavía, si se interpreta aquel ilícito como un tipo mutilado en dos actos,[34] lo relevante será que el hechor, mediante engaño, obtenga ciertas informaciones o vulnere determinadas medidas de seguridad para, con posterioridad, suplantar al titular o usuario y efectuar pagos o transacciones electrónicas; sin que sea necesario que esto último se verifique para entender consumado el delito. Aquí radica la segunda gran diferencia entre el ilícito de la Ley 20.009 y el fraude informático: sólo este último requiere la provocación de un perjuicio patrimonial ajeno para que se perfeccione el tipo penal.

Por último, el delito del artículo 7, inciso segundo, de la Ley 20.009 no establece exigencias subjetivas particulares, de lo cual se sigue que puede cometerse con dolo eventual, así como que no es indispensable que el autor actúe con un ánimo especial al ejecutar la conducta incriminada. Por su parte, y según profundizaremos *infra*, el fraude informático supone una manipulación de datos de sistemas informáticos, que genera un daño patrimonial ajeno y que es llevada a cabo con el ánimo de obtener un lucro (ilegítimo). Ello puede explicarse, al menos en parte, porque el delito de uso fraudulento de tarjetas de pago y transacciones electrónicas, sancionado en el artículo 7, no tiene una connotación exclusivamente patrimonial y, por el contra-

33. Véase, con referencia a la estafa, Mayer (2014: 1.025).

34. Esto es, como un delito en que la intención del agente, al llevar a cabo la conducta típica, debe dirigirse a realizar otra actividad posterior del mismo sujeto. Véase Mir Puig (2016: 235).

rio, también afecta a otros bienes jurídicos, entre los que destaca la funcionalidad documental.[35]

Sobre la base de lo señalado, es posible confirmar lo aseverado al comienzo de este acápite: el tipo del artículo 7, inciso segundo, de la Ley 20.009 se relaciona con el fraude informático en sentido estricto en atención a su contexto comisivo y al hecho de que ambos impliquen la utilización de tecnologías para su perpetración. En cambio, dichos delitos se diferencian en relación con su estructura típica, con su objeto material y con los elementos subjetivos que han de concurrir en uno y otro caso.

## Propuestas para la regulación del fraude informático

### El fraude informático en el CCCE

El año 2017 el Estado chileno pasó a ser parte del Convenio sobre Ciberdelincuencia del Consejo de Europa, razón que lleva a tener en cuenta lo establecido en dicho instrumento internacional en materia de criminalidad informática, sobre todo de cara a una eventual reforma legislativa de su actual regulación.

Como es sabido, el CCCE, dentro del apartado destinado al «Derecho penal sustantivo», establece una sistematización de diversos comportamientos delictivos,[36] que agrupa de la siguiente manera:

- Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, que abarcan el acceso ilícito, la interceptación ilícita, los ataques a la integridad de los datos, los ataques a la integridad del sistema y el abuso de los dispositivos (artículos 2 a 6).
- Delitos informáticos, entre los que se cuentan la falsificación informática y el fraude informático (artículos 7 y 8).
- Delitos relacionados con el contenido, que se extienden únicamente a los delitos vinculados con la pornografía infantil (artículo 9).

35. Ello es bastante claro tratándose de la falsificación de tarjetas de pago; o del uso, de la venta, exportación, importación o distribución de tarjetas de pago falsificadas.

36. Se trata de una sistematización curiosa, cuyo criterio de ordenación no resulta para nada evidente. En ese sentido, mientras que los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, y los delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines parecen tener en cuenta el bien jurídico afectado; los delitos informáticos evocarían un medio o contexto de comisión; mientras que los delitos relacionados con el contenido se centrarían en el objeto material del comportamiento. Otra cuestión que resulta llamativa y que aleja la sistemática del CCCE de la manera en que doctrinalmente se clasifican los delitos informáticos, es que sólo se denomine «delitos informáticos» a los comportamientos constitutivos de falsificación informática y de fraude informático. Lo anterior, por cierto, plantea la duda de si acaso las restantes figuras delictivas, que describe el CCCE, tienen o no esa naturaleza, o si, por el contrario, ella sólo puede predicarse de los referidos ilícitos.

- Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines, entre los que se incluyen, justamente, los delitos contra la propiedad intelectual y los derechos afines (artículo 10).

Como es propio de esa clase de instrumento internacional —y así se desprende de la rúbrica del capítulo 2 sobre «Medidas que deberán adoptarse a nivel nacional»—, los Estados que han suscrito el CCCE han de considerar tales descripciones e incorporarlas, de alguna manera, en su normativa interna. Lo anterior, por cierto, favorece la existencia de respuestas uniformes o al menos similares de los Estados parte en esta materia, y puede impactar de manera indirecta a los Estados que no lo han firmado, pero que, de todos modos, lo consideran por ser el principal instrumento internacional que regula la cibercriminalidad. De ahí la importancia de tener en cuenta las descripciones previstas en el CCCE respecto de los delitos informáticos en general y del fraude informático en particular.

Pues bien, de acuerdo con el artículo 8 del CCCE,

> 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.

De la lectura del referido artículo 8 se desprende que el fraude informático es entendido como una figura de lesión patrimonial; más precisamente, él puede ser interpretado como un delito en que el perjuicio patrimonial de otro es ocasionado a través de determinados medios «informáticos».

El hecho de que se aluda expresamente a la provocación de un perjuicio patrimonial destaca el injusto subyacente al fraude informático: dicho delito, como ocurre con varios otros que se tipifican en nuestra legislación (por ejemplo, la estafa o la administración desleal), afecta el (activo del) patrimonio de la víctima, o sea una universidad jurídica (Politoff, Matus y Ramírez, 2011: 414); no así la propiedad, esto es, «el especial vínculo que existe entre una cosa y el titular de un derecho de exclusión sobre ella» (Hernández Basualto, 2005: 240), como paradigmáticamente ocurre en el delito de hurto.

En relación con el perjuicio patrimonial exigido, el CCCE establece claramente que el fraude informático es un delito de resultado, toda vez que requiere causar un daño en intereses patrimoniales ajenos a través de determinadas conductas. Por lo mismo, implica que se verifiquen los elementos comunes a la estructura típica de los delitos de resultado, como son: la ejecución de un comportamiento delictivo, la

provocación de un resultado típico y la existencia de un vínculo causal entre ese comportamiento y ese resultado.

Asimismo, la exigencia de provocación de un perjuicio patrimonial sugiere que nos hallamos ante un delito de daño efectivo de intereses patrimoniales ajenos, en que, por ende, no se reprime la sola puesta en peligro del patrimonio de otra persona.

En lo que atañe al medio para la provocación del perjuicio patrimonial ajeno, el CCCE contempla diversas modalidades de ejecución que pueden orientarse a causarlo, a saber, la introducción, alteración, borrado o supresión de datos informáticos, o bien, cualquier interferencia en el funcionamiento de un sistema informático. Por lo tanto, el fraude informático es regulado como un delito con pluralidad de hipótesis alternativas, en el sentido de que él describe cinco medios comisivos, cualquiera de los cuales puede dar lugar a su perpetración.

Respecto de tales modalidades ejecutivas, es posible efectuar algunas observaciones:

En primer lugar, que el CCCE no limita el fraude informático a la manipulación o alteración de datos informáticos[37] e incluye, en cambio, medios comisivos que más bien lo acercan al sabotaje informático, como son la introducción y muy especialmente el borrado o supresión de datos;[38] a lo que se agrega la interferencia en el funcionamiento del sistema, que también puede asociarse con el tipo de sabotaje.[39]

En segundo lugar, resulta llamativo que se contemplen tanto modalidades de ejecución que afectan a los datos (introducción, alteración, borrado o supresión) como medios comisivos que inciden en el funcionamiento del sistema informático (interferencia). En esta materia, habría que dilucidar si existe algún caso de interferencia del sistema que no implique, en algún sentido, introducción, alteración, borrado o supresión de datos; así como si se trata de modalidades ejecutivas equivalentes desde el punto de vista del desvalor de acción.

En tercer lugar, aunque el artículo 8 del CCCE parece limitar la intención de ob-

37. En cambio, entiende que el concepto de manipulación informática debe ser interpretado como sinónimo de los cinco comportamientos previstos en el CCCE, Faraldo Cabana (2007: 41-42).

38. En ese sentido, en el artículo 4 número 1 del CCCE se describen los «ataques a la integridad de los datos», noción que en el fondo incluye supuestos de sabotaje informático (De la Mata Barranco y Hernández Díaz, 2010: 161; Jijena Leiva, 2008: 149), ya que con ella se plantea el castigo de «todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos», para lo cual es relevante en este caso la referencia al borrado o supresión de los datos.

39. En esa línea, en el artículo 5 del CCCE se describen los «ataques a la integridad del sistema», noción que en el fondo abarca hipótesis de sabotaje informático (De la Mata Barranco y Hernández Díaz, 2010: 161; Jijena Leiva, 2008: 149), toda vez que con ella se plantea sancionar «la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos», para lo cual es relevante en este caso la referencia a la obstaculización del funcionamiento del sistema por alguno de los medios señalados.

tener un beneficio económico (o ánimo de lucro) tan solo al caso en que existe interferencia en el funcionamiento de un sistema informático, no se divisan razones para efectuar semejante restricción. Por el contrario, como veremos luego, una regulación adecuada del fraude informático debería considerar el ánimo de lucro ante cualquier modalidad comisiva, ya sea de manera explícita o como elemento conceptualmente implicado en la descripción de que se trate.

## Directrices para la (eventual) tipificación del delito de fraude informático

A la luz de lo planteado *supra,* es posible sostener que la regulación del fraude informático en el ordenamiento jurídico chileno debería girar en torno a los tres siguientes requisitos copulativos; dos de ellos integran la tipicidad objetiva, uno de ellos, la subjetiva. Nos referimos a la conducta típica consistente en «manipular» o «alterar» datos de sistemas informáticos y al resultado típico que importa provocar un «perjuicio patrimonial» ajeno mediante ese comportamiento; así como a la existencia de un ánimo o tendencia interna trascendente particular, que se identifica con la motivación de lucro del agente.

En nuestra opinión, esas tres exigencias deben presentarse en conjunto, pues, de faltar alguna de ellas, se corre el riesgo de confundir al fraude informático con otros comportamientos delictivos que integran la Parte Especial. Al mismo tiempo, el hecho de agregar un elemento subjetivo a la noción de fraude informático nos permite precisar la primera aproximación a dicho delito, señalada *supra*, que ahora definimos como la manipulación o alteración de datos o programas de sistemas informáticos, que provoca un perjuicio patrimonial y es realizada con ánimo de lucro. Seguimos, por consiguiente, muy de cerca el concepto de fraude informático que Romeo Casabona (1988: 47) postuló hace más de tres décadas (véase igualmente Balmaceda Hoyos, 2009: 115) y cuya vigencia, a pesar de los cambios que ha experimentado la informática en el último tiempo, se mantiene intacta.

### *Fraude informático y manipulación o alteración de datos*

La vinculación que se ha planteado entre el fraude informático y otros delitos de la Parte Especial permite constatar que aquello que lo distingue de otros ilícitos es el medio de afectación de intereses patrimoniales ajenos, esto es, la manipulación o alteración de datos o programas de sistemas informáticos.

*Alterar*, de acuerdo con su sentido natural y obvio, implica cambiar la esencia o forma de algo, mientras que *manipular* puede interpretarse como intervenir una cosa, distorsionándola.[40] Por tanto, de lo que se trata es de modificar los datos o pro-

40. RAE, *Diccionario de la lengua española*, s. v. «manipular», primera y tercera acepción, disponible

gramas de un sistema de tratamiento automatizado de la información, o bien, de intervenirlos, distorsionando su configuración.

En cuanto a la similitud y relación entre dicha conducta y la de los otros delitos fundamentales que integran la criminalidad informática, debe tenerse presente que manipular y sobre todo alterar los datos puede resultar difícil de distinguir del comportamiento característico del sabotaje informático,[41] que corresponde a destruir o inutilizar datos o programas. Ello es así, porque una de las acepciones de *alterar* es estropear, dañar o descomponer,[42] razón que lleva a no preferirla, precisamente, para posibilitar una delimitación más clara entre el fraude informático y el sabotaje informático.

De otro lado, como se indicó, si se asume que el espionaje informático supone acceder a y conocer (indebidamente) datos de sistemas informáticos, comprobaremos que el delito de fraude informático implica una verificación previa de ese acceso y eventual conocimiento de datos; circunstancia que a su turno obliga a precisar el injusto del espionaje informático recurriendo a otros elementos, entre los que destacan la información sobre la que él recae y el establecimiento de barreras técnicas como señal de exclusión inequívoca (pero no única) de terceros.[43]

Desde el punto de vista del desvalor de acción, o sea, de la gravedad intrínseca de dicho comportamiento, es posible comparar la conducta característica del fraude informático con la de los otros delitos informáticos nucleares (sabotaje informático y espionaje informático) y afirmar que aquélla es más o menos equivalente a éstas en cuanto a su entidad, cuestión que debería considerarse al momento de establecer legislativamente la pena aplicable a tales ilícitos. En ese sentido, puede sostenerse que manipular o alterar datos o programas involucra una gravedad análoga a su destrucción o inutilización; y lo mismo cabe decir si se compara esa manipulación o alteración con el acceso a y eventual conocimiento (indebido) de los datos en cuestión.

Con todo, de estimarse que las conductas propias del sabotaje informático y del espionaje informático son más graves, para efectos penológicos puede compensarse el menor desvalor de acción del fraude informático con su (eventualmente mayor) desvalor de resultado (perjuicio patrimonial) o con otras variables de corte crimino-

---

en https://dle.rae.es/manipular. Sobre la acción consistente en manipular datos, con referencias asimismo al sentido natural y obvio de tal expresión, véase Huerta Miranda y Líbano Manzur (1996: 124).

41. En esa línea, entienden que el sabotaje informático también involucra una alteración de datos, por ejemplo, De la Mata Barranco y Hernández Díaz (2010: 161); Huerta Miranda y Líbano Manzur (1996: 138). En el mismo sentido, a propósito del delito del §303a StGB, denominado por la doctrina, justamente, «alteración de datos», Hilgendorf y Valerius (2012: 176).

42. RAE, *Diccionario de la lengua española*, s. v. «alterar», segunda acepción, disponible en https://dle.rae.es/alterar.

43. Fundamental Medina Schulz (2014: 85, 87-89, 94-97). Véase, asimismo, más recientemente, favoreciendo una interpretación restrictiva de dicha figura, Hernández Basualto (2020).

lógico, como la (posible mayor) frecuencia en la comisión de fraudes informáticos, a veces de gran cuantía económica.

Tratándose de la comparación entre la conducta del fraude informático y delitos como la estafa o el hurto, es posible llegar a conclusiones análogas, o sea, que estamos ante ilícitos de gravedad similar, circunstancia que una vez más debería tomarse en cuenta a la hora de consagrar legalmente la sanción a imponer en cada uno de esos supuestos. En el caso de la estafa, hay una instrumentalización de la víctima que, en términos generales, puede considerarse de entidad equivalente al empleo de medios subrepticios o clandestinos, que muchas veces caracteriza al hurto. Tratándose de este último delito, es evidente que la relativamente mayor frecuencia en su comisión también ha llevado a intensificar la reacción penal frente al mismo, no sin riesgo de penas desproporcionadas.

Como sea, resulta interesante establecer que, desde el punto de vista de la posible interacción con la víctima, el fraude informático ha ido abandonando el contacto con los afectados, muy característico del empleo del *phishing*, para pasar a una fase de afectación directa de los datos a través de un *malware*. Ello hace que su modo de ejecución hoy tenga más de subrepticio o clandestino que de instrumentalización (Faraldo Cabana, 2007: 36-37), lo que a su vez refuerza las diferenciaciones que tradicionalmente se han planteado entre la estafa, por una parte, y el fraude informático, por la otra.

### *Fraude informático y perjuicio patrimonial*

El fraude informático integra el grupo de delitos que afectan intereses patrimoniales ajenos,[44] cuestión que lo acerca claramente a los delitos contra la propiedad, regulados en el título 9 del libro 2 del Código Penal. Como se dijo, tal afectación, unida a la frecuencia de su comisión, explica que el fraude informático se haya convertido en la figura central de la criminalidad informática, actualmente muy relacionada con el comercio electrónico y las transferencias de fondos en línea.

El desvalor de resultado, o sea, la afectación de bienes jurídicos propia del fraude informático se identifica, en todos los casos, con la vulneración del (activo del) patrimonio de la víctima, concepto que, según la doctrina mayoritaria (De la Fuente Hulaud, 2005: 612-613; Politoff, Matus y Ramírez, 2011: 416; Yubero Cánepa, 2010: 54), es entendido en un sentido jurídico-económico (Bascuñán Rodríguez, 2004: 292-293). Mientras que el perjuicio patrimonial, de acuerdo con dicha concepción, puede definirse como «la disminución del valor monetario del patrimonio» (Hernández Basualto, 2008a: 196).

44. Véase, entre muchos otros, Balmaceda Hoyos (2009: 115), Eisele (2013: 168), García García-Cervigón (2008: 294). Con matices, Magliona y López (1999: 203).

Pero, además, cuando un fraude informático es cometido en el ciberespacio, él también afecta al bien jurídico que comparte con otros ciberdelitos, denominado, como se dijo, «funcionalidad informática». En el caso del fraude informático, dicho bien jurídico cobra una relevancia especial, ya que si no todos, la enorme mayoría de los supuestos de defraudación informática que se lleva a cabo utiliza internet como contexto de ejecución del comportamiento delictivo. En ese sentido, mientras que todavía son imaginables y relativamente importantes algunos casos de destrucción de datos (sabotaje informático) o de acceso a y conocimiento indebido de éstos (espionaje informático) sin que se recurra al ciberespacio, no puede decirse lo mismo del fraude informático, que en general se comete en relación con el comercio electrónico y de las transferencias de fondos en línea.

Dicha circunstancia provoca que el fraude informático por lo general sea un delito pluriofensivo, pues afecta a un bien jurídico individual, que corresponde a intereses patrimoniales ajenos; y a un bien jurídico supraindividual, que se identifica con las condiciones que permiten que los sistemas de tratamiento automatizado de la información ejecuten de manera adecuada las operaciones de almacenamiento, tratamiento y transferencia de datos, dentro de un marco tolerable de riesgo.

Ahora bien, tal carácter pluriofensivo se ha de tener en cuenta al momento de regular expresamente el delito de fraude informático en la legislación chilena y puede, en su caso, reforzar la equivalencia de dicho ilícito con otros delitos de la Parte Especial (por ejemplo, la estafa o el hurto), cuyos medios de comisión o frecuencia práctica pudieran justificar una sanción más drástica.

Finalmente, a propósito de este último punto y ante el aumento probable de fraudes informáticos en el futuro, debido al incremento de las relaciones negociales a través de internet, sería esperable que ese delito tuviera una pena que considerara tanto su gravedad dentro del sistema de los delitos informáticos (o sea, en relación con el sabotaje y el espionaje informático); pero también dentro del sistema de delitos de la Parte Especial (esto es, respecto de figuras delictivas más o menos similares, y muy especialmente de la estafa y del hurto).

### *Fraude informático y ánimo de lucro*

Hasta ahora el análisis que se ha efectuado del fraude informático ha apuntado fundamentalmente a su injusto y, en vinculación con ello, a aspectos objetivos de dicho ilícito, en concreto, a su conducta y resultado. No obstante, los delitos que afectan intereses patrimoniales pueden, también, contener elementos subjetivos especiales, que permiten perfilar de mejor manera el sentido del comportamiento y el castigo asociado a éste.

En este contexto, si se tiene en cuenta la clasificación de los delitos contra intereses patrimoniales que se centra en lo que el agente persigue con la comisión de la con-

ducta típica, es posible distinguir entre delitos de enriquecimiento o lucro, por una parte, y delitos de mero perjuicio, por la otra (Oliver, 2013: 33, con referencias ulteriores). El fraude informático integra, precisamente, los primeros, junto con otros ilícitos como la estafa (García García-Cervigón, 2008: 293) y el hurto. Ejemplos de delitos de mero perjuicio, en cambio, son los llamados «delitos de destrucción», entre los que se cuentan, entre otros, los estragos y los daños, así como el sabotaje informático.

La exigencia de ánimo de lucro en relación con el fraude informático es coherente con la fenomenología de dicho delito que, en la práctica, implica efectivamente la persecución de un lucro ilegítimo de parte del agente del comportamiento incriminado (Fernández Teruelo, 2007: 217; Miró Llinares, 2013: 3-4; Romeo Casabona, 1988: 47, 71, 120 y *passim*). En efecto, quienes manipulan datos informáticos para, por ejemplo, posibilitar transferencias de fondos desde la cuenta corriente de la víctima a la cuenta corriente de un tercero, sin la voluntad de la primera ni del banco, lo hacen para obtener un enriquecimiento (propio o ajeno) y no con el simple objeto de dañar los intereses patrimoniales de aquélla.

Por otra parte, el ánimo de lucro posibilita una definición más adecuada del fraude informático en tanto delito informático. En ese orden de cosas, si dicho delito se identifica sólo con la manipulación o alteración (dolosa) de datos de sistemas informáticos, que provoca un daño económico, él no se diferenciaría mayormente de algunas hipótesis de sabotaje informático en las que existe, por ejemplo, alteración, borrado o supresión (dolosos) de datos informáticos que tienen un valor económico (Romeo Casabona, 1988: 175). Es el ánimo de lucro el que le imprime un carácter particular al fraude informático y cuya ausencia impide su configuración, lo que es sin perjuicio de que se verifique algún otro delito informático, en especial, el ya mencionado sabotaje informático (en caso de que, por ejemplo, hubiere habido una alteración de datos con un consiguiente daño patrimonial) o un espionaje informático (por ejemplo, si hubiere habido un acceso a y conocimiento indebido de datos).

El ánimo de lucro permite, asimismo, una mejor delimitación entre el fraude informático y otros delitos de la Parte Especial, como la administración desleal (artículo 470 número 11 del Código Penal), delito en que el agente no actúa con el ánimo de obtener un lucro (ilegítimo), sino con la intención de provocar un mero perjuicio patrimonial a la víctima (Bofill, Jelvez y Contreras, 2019: 74).[45]

A la luz de lo señalado, puede sostenerse un paralelismo, en el plano subjetivo, tanto entre la estafa y el fraude informático (Hilgendorf y Valerius, 2012: 157), por

45. Por cierto, contribuye también a la delimitación entre el fraude informático y delitos como la administración desleal el hecho de que la conducta delictiva del primero se centre en la manipulación de datos, en el sentido indicado *supra*, y no, por ejemplo, en el uso no autorizado o ilícito de datos. Respecto de este asunto, con referencias a la normativa alemana, Gercke (2009: 96).

una parte, como entre el delito de daños y el sabotaje informático,[46] por la otra. En cambio, es posible que el espionaje informático se relacione con diversos móviles o intenciones del hechor, los que a su turno se vincularán con la clase de información a la que indebidamente se accede (militares, industriales, financieras, profesionales, personales, etcétera) y que en su caso se conoce.

## Propuesta de regulación del fraude informático en actual trámite parlamentario (artículo 7 del Boletín 12.192-25)

El proyecto de ley que busca modificar la regulación de los delitos informáticos (Boletín 12.192-25) propuso regular el fraude informático en su artículo 6, según el cual, será castigado

> 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.

La Comisión de Seguridad Pública del Senado introdujo modificaciones a dicha propuesta, que hoy figura en el artículo 7, y sanciona

> al 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.

Si se tiene en cuenta la última versión del precepto, podrá constatarse que la conducta que pretende tipificarse se identifica exclusivamente con manipular un sistema de tratamiento automatizado de la información. En cambio, la introducción, la alteración, el daño o la supresión de datos, o bien, la interferencia en el funcionamiento de un sistema informático constituyen modalidades o medios de ejecución de dicho comportamiento.

Sobre esa base, y en la línea de lo que se indicó al analizar la regulación del fraude informático en el CCCE (que se refiere a la introducción, a la alteración, al borrado o a la supresión de datos), algunas de las modalidades previstas para la tipificación del fraude informático se acercan mucho a la conducta que es característica del sabotaje informático. Así ocurre tratándose del medio comisivo que se identifica con la introducción de datos y —muy en particular— con el que supone un daño o supresión de datos de sistemas informáticos.

46. Sobre la relación entre estos últimos delitos, aunque con matices relativos a la denominación de los comportamientos incriminados, De la Mata Barranco y Hernández Díaz (2010: 161), Hilgendorf y Valerius (2012: 176), Oliver (2013: 553-554) y Picotti (2013: 46).

Por otra parte, la consagración de cinco modalidades de ejecución respecto de una conducta, como la de manipular, envuelve el riesgo de dejar impunes comportamientos que no sean ejecutados a través de alguno de los medios expresamente descritos. La cláusula final, que alude a «cualquier interferencia en el funcionamiento de un sistema informático», si bien aparece redactada en el sentido de una hipótesis residual, en el fondo castiga a quien «manipule un sistema informático, mediante […] cualquier interferencia en el funcionamiento de un sistema informático». En ese orden de ideas, el hecho de no recaer explícitamente sobre datos hace que esta última modalidad sea una más, alternativa a las restantes, pero no una cláusula genérica capaz de captar medios específicos indicados con anterioridad.

Frente a ello, así como en miras a simplificar una redacción innecesariamente alambicada, sería preferible centrar el castigo en la conducta consistente en manipular datos o programas de un sistema de tratamiento automatizado de la información, que resulta lo suficientemente comprensiva como para abarcar los comportamientos constitutivos de fraude informático en sentido estricto.

De otro lado, a fin de destacar de manera adecuada que la manipulación de datos es el medio para provocar el resultado de perjuicio patrimonial ajeno, sería recomendable que este último figurara al final de la descripción, y no al principio de ella, como se señala en la propuesta. En relación con este punto, también resultaría deseable exigir que la conducta cause un perjuicio patrimonial o perjudique patrimonialmente y no que se verifique cuando o mientras se está «causando» ese resultado material.

Además, la referencia expresa a la finalidad de obtener un beneficio económico para sí o para un tercero podría describirse en términos más acordes con nuestra tradición legislativa (por ejemplo, en materia de hurto y robo), o sea, como una exigencia de ánimo de lucro. De todos modos, debe celebrarse la aclaración en orden a que el provecho perseguido pueda ser para el agente o para un sujeto distinto de él, así como que se aluda abiertamente a su naturaleza económica, lo que es coherente con la forma de establecer la penalidad y destaca el sentido defraudatorio —y no solamente informático— del tipo penal.

Por último, la pena contemplada para el fraude informático es casi idéntica a la del delito de estafa, lo que expresa una intención de castigarlo como una figura paralela a aquel tipo penal. La diferencia se produce en las hipótesis de menor gravedad, ya que mientras la estafa recién pasa a constituir un simple delito cuando el monto de lo defraudado excede de una unidad tributaria mensual —en cuyo caso se aplica la pena de presidio menor en su grado mínimo y multa de cinco unidades tributarias mensuales (artículo 467 número 3, en relación con artículo 494 número 19 del Código Penal)—, en el proyecto de ley se pretende aplicar la pena de presidio menor en su grado mínimo y multa de cinco a diez unidades tributarias mensuales si el valor del perjuicio no excediere de cuatro unidades tributarias mensuales.

Las razones de tal diferenciación no son evidentes y no pueden hallarse en la

eventual pluriofensividad del fraude informático cometido mediante redes computacionales. Pues, de haberse considerado lo anterior, habría tenido que establecerse en general una pena mayor para los comportamientos correspondientes a fraudes informáticos ejecutados a través de internet. De otro lado, el hecho de sancionar fraudes informáticos de muy baja cuantía plantea el problema, más amplio, relativo a si y cómo castigar penalmente supuestos de delincuencia informática de bagatela, cuestión que ciertamente excede las pretensiones del presente artículo.

## Conclusiones

A pesar del interés teórico que genera el fraude informático, así como de la importancia práctica que tiene dicho delito, aún no existe total claridad respecto de qué implica con exactitud cometer una conducta que pueda calificarse de tal.

Si se consideran en particular los problemas que plantea la delimitación entre ese ilícito y otros comportamientos, eventualmente punibles, se advertirá que muchas veces se incluyen dentro de la noción de fraude informático conductas que en realidad corresponden a etapas de ejecución imperfecta (delito tentado o frustrado) e incluso a actos preparatorios de un fraude propiamente tal, como ocurre con los comportamientos de *phishing* y *pharming*; o bien, que se denomina fraude informático a conductas que en verdad corresponden a otros delitos informáticos, entre los que destaca el espionaje informático (o *hacking*) y el sabotaje informático.

A fin de favorecer una adecuada definición y delimitación del fraude informático, que tenga en cuenta el papel que cumple en el sistema de los delitos informáticos, así como más ampliamente al interior de la Parte Especial, se concluye la necesidad de regular dicho delito en torno a tres requisitos copulativos: primero, la verificación de la conducta típica consistente en «manipular» datos o programas de sistemas de tratamiento automatizado de la información; segundo, la provocación de un resultado típico, que se identifica con un «perjuicio patrimonial» ajeno; y, tercero, la presencia de «ánimo de lucro» en el agente del comportamiento incriminado.

Con ello, se afirma la conveniencia de precisar algunas de las directrices contenidas en el artículo 8 del CCCE para la tipificación del fraude informático, a la hora de emprender la regulación expresa de dicho delito en el ordenamiento jurídico penal chileno.

## Agradecimientos

Trabajo redactado en el marco del proyecto Fondecyt núm. 1161066: «Los delitos informáticos en el ordenamiento jurídico chileno: Análisis dogmático y crítico, y propuestas *de lege ferenda*».

## Referencias

Aguilar Aranela, Cristian (2008). *Delitos patrimoniales*. Santiago: Metropolitana.

Agustina, José (2009). «La arquitectura digital de internet como factor criminógeno: Estrategias de prevención frente a la delincuencia virtual». *International E-Journal of Criminal Sciences*, 3: 1-31. Disponible en https://bit.ly/3iavH6U.

Anderson, Keith B., Erik Durbin y Michael A. Salinger (2008). «Identity theft». *Journal of Economic Perspectives*, 22 (2): 171-192. DOI: 10.1257/jep.22.2.171.

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

Bascuñán Rodríguez, Antonio (2004). «Delitos contra intereses instrumentales». *Revista de Derecho de la Universidad Adolfo Ibáñez*, 1: 291-345.

Bofill, Jorge, Valeria Jelvez y Sebastián Contreras (2019). «Consideraciones sobre el nuevo delito de administración desleal en el derecho chileno». *Derecho & Sociedad*, 52: 59-77. Disponible en https://bit.ly/2Zd949j.

Brody, Richard, Elizabeth Mulig y Valerie Kimball (2007). «Phishing, pharming and identity theft». *Academy of Accounting and Financial Studies Journal*, 11 (3): 43-56. Disponible en https://bit.ly/2B8HzWG.

Brunst, Phillip (2009). *Anonymität im Internet: Rechtliche und tatsächliche Rahmenbedingungen*. Berlín: Duncker & Humblot.

Bullemore, Vivian y John Mackinnon (2018). *Curso de derecho penal, parte especial*. Tomo 4. Santiago: Ediciones Jurídicas de Santiago.

Cury, Enrique (2011). *Derecho penal, parte general*. Santiago: Ediciones UC.

De la Fuente Hulaud, Felipe (2005). «Delitos contra intereses instrumentales». *Revista de Derecho de la Universidad Adolfo Ibáñez*, 2: 557-617.

De la Mata Barranco, Norberto y Leyre Hernández Díaz (2010). «Los delitos vinculados a la informática en el derecho penal español». En José Luis de la Cuesta Arzamendi (director), *Derecho penal informático* (pp. 159-200). Madrid: Civitas.

Eisele, Jörg (2013). *Computer- und Medienstrafrecht*. Múnich: Beck.

Escalona Vásquez, Eduardo (2004). «El *hacking* no es (ni puede ser) delito». *Revista Chilena de Derecho Informático*, 4: 149-167. DOI: 10.5354/0717-9162.2011.10678.

Etcheberry, Alfredo (2010). *Derecho penal, parte especial*. Tomo 3. Santiago: Jurídica de Chile.

Faraldo Cabana, 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/3eKRhx2.

Fernández Teruelo, Javier (2011). *Derecho penal e internet*. Valladolid: Lex Nova.

—. (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. Disponible en https://bit.ly/3eGbjsb.

Flores Mendoza, Fátima (2014). «Respuesta penal al denominado robo de identidad en las conductas de *phishing* bancario». *Estudios Penales y Criminológicos*, 34: 301-339. Disponible en https://bit.ly/384wxNY.

García García-Cervigón, Josefina (2008). «El fraude informático en España e Italia: Tratamiento jurídico-penal y criminológico». *Icade*, 74: 289-308. Disponible en https://bit.ly/2Nw7av4.

Garrido Montt, Mario (2011). *Derecho penal, parte especial*. Tomo 4. Santiago: Jurídica de Chile.

Gercke, Marco (2009). «Kapitel 3: Materielles Strafrecht». En Marco Gercke y Phillip Brunst. *Praxishandbuch Internetstrafrecht* (pp. 58-231). Stuttgart: Kohlhammer.

Gercke, Marco y Phillip Brunst (2009). *Praxishandbuch Internetstrafrecht*. Stuttgart: Kohlhammer.

Gillespie, Alisdair (2016). *Cybercrime: Key issues and debates*. Nueva York: Routledge.

Grabosky, Peter (2009). «High tech crime: Information and communication related crime». En Hans Joachim Schneider (editor), *Internationales Handbuch der Kriminologie* (pp. 73-101). Tomo 2. Berlín: De Gruyter.

Gutiérrez Francés, María Luz (1991). *Fraude informático y estafa: Aptitud del tipo de estafa en el derecho español ante las defraudaciones por medios informáticos*. Madrid: Ministerio de Justicia, Secretaría General Técnica, Centro de Publicaciones.

Hermosilla, Juan Pablo y Rodrigo Aldoney (2002). «Delitos informáticos». En Íñigo de la Maza (coordinador), *Derecho y tecnologías de la información* (pp. 415-429). Santiago: Fundación Fernando Fueyo, UDP.

Hernández Basualto, Héctor (2001). «Tratamiento de la criminalidad informática en el derecho penal chileno: Diagnóstico y propuestas». Informe solicitado por la División Jurídica del Ministerio de Justicia. Inédito.

—. (2003). «Aproximación a la problemática de la estafa». En *Problemas actuales de derecho penal* (pp. 147-190). Temuco: Universidad Católica de Temuco.

—. (2005). «La administración desleal en el derecho penal chileno». *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, 26: 201-258. Disponible en https://bit.ly/31z6moX.

—. (2008a). «Frustración de fines y perjuicio patrimonial en el derecho penal chileno». En José Ángel Fernández (coordinador), *Estudios de ciencias penales: Hacia una racionalización del derecho penal* (pp. 195-223). Santiago: Legal Publishing.

—. (2008b). «Uso indebido de tarjetas falsificadas o sustraídas y de sus claves». *Revista Política Criminal*, 3 (5): 138. Disponible en https://bit.ly/2Bix6rv.

—. (2010). «Por qué no puede prescindirse de la exigencia de error en la estafa». *Revista Doctrina y Jurisprudencia Penal*, 1: 29-41.

—. (2020). «Der unbefugte Zugang zu einem Computersystem und die Grenzen des zu beachtenden Willens des Rechtsinhabers». *FS-Sieber* (en prensa): 1-9.

Herzog, Felix (2009). «Straftaten im Internet, Computerkriminalität und die Cy-

bercrime Convention». *Política Criminal*, 4 (8): 475484. Disponible en https://bit.ly/2CNM3T1.

Hilgendorf, Eric y Brian Valerius (2012). *Computer- und Internetstrafrecht*. Heidelberg: Springer.

Hong, Haeji (1997). «Hacking through the Computer Fraud and Abuse Act». *UC Davis Law Review*, 31: 283-307. Disponible en https://bit.ly/310Crsa.

Huerta Miranda, Marcelo y Claudio Líbano Manzur (1996). *Delitos informáticos*. Santiago: Jurídica ConoSur.

Jijena Leiva, Renato (1992). *Chile, la protección penal de la intimidad y el delito informático*. Santiago: Jurídica de Chile.

—. (1993). «Debate parlamentario en el ámbito del derecho informático: Análisis de la Ley 19.223, de junio de 1993, que tipifica delitos en materia de sistemas de información». *Revista de Derecho de la Universidad Católica de Valparaíso*, 15: 347-401. Disponible en https://bit.ly/310CUKW.

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

Kaiser, Günther (1996). *Kriminologie: Ein Lehrbuch*. Heidelberg: C. F. Müller.

Kindhäuser, Urs (1999). «Der Computerbetrug (§ 263a StGB) – ein Betrug?». En Erich Samson, Friedrich Dencker, Peter Frisch, Helmut Frister y Wolfram Reiß (editores), *Festschrift für Gerald Grünwald* (pp. 285-305). Baden-Baden: Nomos.

Kochheim, Dieter (2015). *Cybercrime und Strafrecht in der Informations-und Kommunikationstechnik*. Múnich: Beck.

Krombholz, Katharina, Heidelinde Hobel, Markus Huber y Edgar Weippl (2014). «Advanced social engineering attacks». *Journal of Information Security and Applications*, 22: 113-122. DOI: 10.1016/j.jisa.2014.09.005.

López, Macarena (2002). «Ley 19.223 y su aplicación en los tribunales». En Íñigo de la Maza (coordinador), *Derecho y tecnologías de la información* (pp. 397-414). Santiago: Fundación Fernando Fueyo, UDP.

Magliona, Claudio (2002). «Análisis de la normativa sobre delincuencia informática en Chile». En Íñigo de la Maza (coordinador), *Derecho y tecnologías de la información* (pp. 383-395). Santiago: Fundación Fernando Fueyo, UDP.

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

Mañalich, Juan Pablo (2018). «Apropiación y distracción indebidas: Una propuesta de reconstrucción unificadoramente dualista del art. 470 n.º 1 del Código Penal». *Revista de Derecho, Universidad Católica del Norte*, 1: 153-180. Disponible en https://bit.ly/2ZeJC3d.

Masís Solís, Jonathan (2016). «El delito de espionaje informático en el derecho internacional y costarricense: Una modalidad de infracción del derecho

humano de la intimidad». *Anuario de Derechos Humanos*, 12: 103-118. DOI: 10.5354/0718-2279.2016.42744.

Mayer, Laura (2014). «El engaño concluyente en el delito de estafa». *Revista Chilena de Derecho*, 41 (3): 1.017-1.048. DOI: 10.4067/S0718-34372014000300010.

—. (2017). «El bien jurídico protegido en los delitos informáticos». *Revista Chilena de Derecho*, 44 (1): 235-260. DOI: 10.4067/S0718-34372017000100011.

—. (2018). «Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos». *Ius et Praxis*, 24 (1): 159-206. DOI: 10.4067/S0718-00122018000100159.

Medina Schulz, Gonzalo (2014). «Estructura típica del delito de intromisión informática». *Revista Chilena de Derecho y Tecnología*, 3 (1): 79-99. DOI: 10.5354/0719-2584.2014.32221.

Miró Llinares, Fernando (2012). *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio*. Madrid: Marcial Pons.

—. (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/3eFtoqy.

Mir Puig, Santiago (2016). *Derecho penal, parte general*. Barcelona: Reppertor.

Moscoso Escobar, Romina (2014). «La Ley 19.223 en general y el delito de *hacking* en particular». *Revista Chilena de Derecho y Tecnología*, 1 (3): 11-78. DOI: 10.5354/0719-2584.2014.32220.

Norris, Gareth, Alexandra Brookes y David Dowell (2019). «The psychology of internet fraud victimisation: A systematic review». *Journal of Police and Criminal Psychology*, 34: 231-245. DOI: 10.1007/s11896-019-09334-5.

Oliver, Guillermo (2013). *Delitos contra la propiedad*. Santiago: Legal Publishing.

Oxman, Nicolás (2013). «Estafas informáticas a través de internet: Acerca de la imputación penal del *phishing* y el *pharming*». *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, 41: 211-262. DOI: 10.4067/S0718-68512013000200007.

Picotti, Lorenzo (2013). «La tutela penale della persona e le nuove tecnologie dell'informazione». En Lorenzo Picotti (editor). *Tutela penale della persona e nuove tecnologie* (pp. 29-75). Padua: Cedam.

Politoff, Sergio, Jean Pierre Matus y María Cecilia Ramírez (2011). *Lecciones de derecho penal chileno, parte especial*. Santiago: Jurídica de Chile.

Quintero Olivares, Gonzalo (2001). «Internet y propiedad intelectual». *Cuadernos de Derecho Judicial*, 10: 367-398.

Romeo Casabona, Carlos María (1988). *Poder informático y seguridad jurídica: La función tutelar del derecho penal ante las nuevas tecnologías de la información*. Madrid: Fundesco.

Rosenblut, Verónica (2008). «Punibilidad y tratamiento jurisprudencial de las conductas de *phishing* y fraude informático». *Revista Jurídica del Ministerio Público*, 35: 254-266.

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

Salvadori, Iván (2010). «La lucha contra el hurto de identidad: Las diferentes perspectivas legislativas». *Revista Holística Jurídica*, 8: 61-78. Disponible en https://bit.ly/2A9CoGN.

San Juan, César, Laura Vozmediano y Anabel Vergara (2009). «Miedo al delito en contextos digitales: Un estudio con población urbana». *Eguzkilore*, 23: 175-190.

Sieber, Ulrich (2014). «§ 24 Computerkriminalität». En Ulrich Sieber, Helmut Satzger y Bernd Heintschel-Heinegg (editores), *Europäisches Strafrecht* (pp. 435-468). Baden-Baden: Nomos.

Suárez Sánchez, Alberto (2009). *La estafa informática*. Bogotá: Ibáñez.

Tiedemann, Klaus (2011). *Wirtschaftsstrafrecht Besonderer Teil*. Múnich: Vahlen.

Yubero Cánepa, Julio (2010). *El engaño en el delito de estafa: Doctrina y jurisprudencia*. Santiago: Jurídica Cruz del Sur.

## Sobre los autores

Laura Mayer Lux es abogada. Licenciada en Ciencias Jurídicas por la Pontificia Universidad Católica de Valparaíso, Chile. Doctora en Derecho por la Universidad de Bonn, Alemania. Profesora de Derecho Penal del Departamento de Derecho Penal y Procesal Penal de la Pontificia Universidad Católica de Valparaíso. Su correo electrónico es laura.mayer@pucv.cl. ORCID: https://orcid.org/0000-0003-1968-6578.

Guillermo Oliver Calderón es abogado. Licenciado en Ciencias Jurídicas por la Pontificia Universidad Católica de Valparaíso, Chile. Magíster en Derecho Penal y Ciencias Penales por las Universidades de Barcelona y Pompeu Fabra, España. Doctor en Derecho, Universidad de Barcelona, España. Profesor de Derecho Penal y Procesal Penal del Departamento de Derecho Penal y Procesal Penal de la Pontificia Universidad Católica de Valparaíso. Su correo electrónico es guillermo.oliver@pucv.cl. ORCID: https://orcid.org/0000-0003-4485-1870.

**REVISTA CHILENA DE DERECHO Y TECNOLOGÍA**

La *Revista de Chilena de Derecho y Tecnología* es una publicación académica semestral del Centro de Estudios en Derecho Informático 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.

EDITOR GENERAL
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).