Revista de Derecho (Valparaiso)
ISSN: 0716-1883
dirder@ucv.cl
Pontificia Universidad Católica de Valparaíso
Chile

Oxman, Nicolás
Estafas informáticas a través de Internet: acerca de la imputación penal del “phishing” y el “pharming”
Revista de Derecho (Valparaiso), núm. XLI, diciembre, 2013, pp. 211-262
Pontificia Universidad Católica de Valparaíso
Valparaíso, Chile

Revista de Derecho
de la Pontificia Universidad Católica de Valparaíso
XLI (Valparaíso, Chile, 2013, 2do Semestre)
[pp. 211 - 262]

Estafas informáticas a través de Internet: acerca de la imputación penal del "phishing" y el "pharming"

[Cybercrime Through Internet: on the Accusation of "Phishing" and "Pharming"]

Nicolás Oxman*
Universidad Santo Tomás, Santiago de Chile

Resumen

Este trabajo aborda la imputación penal de los fraudes informáticos de apoderamiento patrimonial más comunes en Chile. Teniendo en cuenta las posibilidades que ofrece el derecho comparado, se tratan el "phishing" y el "pharming" como tipos de estafa informática.

Palabras clave

"Phishing – "Pharming" – "Money-mules".

Abstract

This work addresses the most common accusations of phishing in Chile. Bearing in mind the possibilities offered by the Comparative Law, "phishing" and "pharming" are analyzed as types of cybercrime.

Keywords

"Phishing – "Pharming" – "Money-mules".

Recibido el 29 de julio y aceptado el 30 de noviembre de 2013

---

* Doctorando en Derecho Penal por la Universidad de Valencia y Magíster en Derecho Penal por la Universidad de Talca; Máster en Derecho Penal por la Universidad de Lérida y Jaume I; profesor de Derecho Penal en la Universidad Santo Tomás. Dirección Postal: Avenida Valladolid, 26, puerta 9, Valencia, España (46020). Dirección electrónica: nicolás.oxman@uv.es. Este trabajo ha sido posible gracias al apoyo económico de la Universidad Santo Tomás (Chile), a través de un proyecto I+D/DIP 68/2011, además, de la colaboración que me ha prestado el Departamento de Derecho Penal de la Universidad de Valencia. Al mismo tiempo, como siempre me debo a la Universidad de Talca y su Centro de Estudios de Derecho Penal. Agradezco a la distancia también a los amigos, en especial, a la Profesora Luz María Vergara y al Profesor Marco Martínez Lazcano e indirectamente a la Unidad de Estudios de la Defensoría Penal Pública de Valparaíso. Finalmente, a Hermán Apablaza e Israel Villavicencio.

I. Introducción

En la actual sociedad de la información la denominada "cibercriminalidad" se presenta en la cotidianeidad de las personas bajo las más variadas formas, expresivas de una amplia heterogeneidad de nuevos fenómenos delictivos y renovadas modalidades de comisión de los delitos tradicionales, especialmente, a través de sistemas o redes informáticas de transmisión e intercambio de datos por Internet, cuya complejidad operativa dificulta su persecución y, consecuentemente, incrementa los niveles de impunidad[1]. Y, aunque en realidad, no exista un concepto de "cirbercriminalidad" unánimemente aceptado, podríamos decir que se trata de un término que hace referencia a un conjunto de actividades ilícitas cometidas al amparo del uso y el abuso de las tecnologías de la información y la comunicación (Tics), poniendo en peligro o lesionado intereses o bienes jurídicos de naturaleza individual, o bien, amenazando la seguridad de los sistemas sociales[2].

---

[1] Sobre este punto, resulta expresiva de la situación actual la idea de que ya no estamos en presencia de ese "hacker romántico" que operaba de modo solitario, sino que, ante una enorme industria del crimen organizado que gira en torno a la informática, vulnerando la seguridad de los sistemas de trasmisión de datos de terceros. Se trata de una cuestión que requiere de una respuesta a través de normativas unificadas de nivel internacional. En efecto, sin perjuicio de las medidas que puedan adoptar en el plano interno los Estados, se requiere de una estrategia unificada con unos marcos penales mínimos, que resuelva entre otros los problemas relativos a la competencia jurisdiccional, que consagre acciones conjuntas y facilite la cooperación internacional en materia penal. Ello, conllevaría la disminución de los altos niveles de impunidad de los ataques informáticos que obran al amparo de las dificultades de persecución penal internacional. Ampliamente, con referencias, González Cussac, José Luis, *Tecnocrimen*, en González Cussac, José Luis - Cuerda Arnau, María Luisa (directores) y Fernández Hernández, Antonio (coordinador), *Nuevas amenazas a la seguridad nacional*: *terrorismo*, *criminalidad organizada y tecnologías de la información y la comunicación* (Valencia, Tirant lo Blanch, 2013), pp. 206-213 y 239 ss.

[2] La idea primigenia de que los delitos cometidos a través de medios informáticos constituyen una nueva forma de criminalidad ha sido sustituida por una concepción según la cual se entiende que acá en realidad existe una complejidad de formas de ataque contra una multiplicidad de intereses de naturaleza individual o colectiva, ya sea al amparo o contra sistemas o datos informáticos de personas físicas o jurídicas. En efecto, en los años setenta y hasta fines de los ochenta del siglo pasado, el contenido del injusto de estas "nuevas formas de criminalidad" se centraba en la explicación de las mismas como ataques a la privacidad. A medida que dichos sistemas se fueron masificando, el foco de la discusión se centró en la conceptualización de estos delitos como "ataques" o "fraudes", o bien, como "espionaje", "manipulaciones" o "destrucción" de sistemas de tratamientos de información o "software" que alojan datos de valor económico (esta es, por ejemplo, la idea del legislador chileno de 1993, a través de la Ley Nº 19.223 que tipifica figuras penales relativas a la informática). Posteriormente, a mediados de los

Dentro de este contexto, nos interesa destacar aquí el particular interés que suscitan en la actualidad los fraudes a la banca electrónica cometidos a través de Internet[3]. Se trata de ataques a la integridad y confidencialidad de los datos personales, y, también, al patrimonio de la entidad bancaria y a la confianza depositada por el titular de la cuenta en la seguridad del sistema financiero para la realización de todo tipo de transacciones civiles y comerciales.

En este orden de ideas, se sostiene que no es suficiente con prevenir estos hechos a través del pago de indemnizaciones civiles a los titulares de las cuentas corrientes[4] y que, al mismo tiempo, no resulta ser bastante la exigencia de seguros, o bien, la mera inversión en educación expresada en la difusión a los usuarios de las más diversas formas en las que se suelen cometer estos

---

años noventa del siglo pasado, con el advenimiento de Internet y la utilización masiva de paquetes de *software* estandarizados por la población, surgieron nuevas formas de violación a la propiedad intelectual, a través de las copias digitales ilegales, principalmente, de música, películas y programas computacionales. Al mismo tiempo, se puso el acento en los contenidos lesivos de intereses especialmente necesitados de protección como ocurrió con la pornografía infantil, las redes de apuesta ilegal o la difusión de contenidos terroristas en la red. A su turno, la utilización por parte de los organismos gubernamentales de Internet los expuso al denominado "terrorismo informático". Para un resumen acerca del desarrollo histórico de este asunto en Europa, puede verse Sieber, Ulrich, *El control de la complejidad en el ciberespacio global*: *a armonización de los delitos informáticos*, en Delmas-Marty, Mireille - Pieth, Mark y otros (directores) y Morales, Marta (coordinadora), *Los caminos de la armonización penal* (Valencia, Tirant Lo Blanch, 2009), pp. 158-161.

[3] Véase, ampliamente, sobre la necesidad de una respuesta penal a los problemas originados en el siglo XXI como consecuencia de la sociedad de la información y la comunicación. Benítez Ortúzar, Ignacio, *Informática y delito*. *Aspectos penales relacionados con las nuevas tecnologías*, en Morillas Cueva, Lorenzo (directores), *Reforma del Código Penal*. *Respuestas para una sociedad del Siglo XXI* (Madrid, Dykinson, 2009), pp. 111 ss.

[4] Al respecto, recientemente, Acum Maldonado, Carolina, *La responsabilidad civil de los prestadores de servicios en la sociedad de la información* en *Revista de Contratación Electrónica*, 115 (2011), pp. 6 ss. Véase, además, la discusión que se dio en el marco de un proceso por infracción a las letras b) y d) del artículo 3 de la Ley Nº 19.496, sobre protección de derechos del consumidor, en el que se consideró que el Banco Santander no debía responder frente a un sujeto que entregó todos los números de su "tarjeta súper clave" a requerimiento de una página "web" duplicada que parecía ser del Banco Santander; la Corte es bastante exigente en cuando a los deberes de información que se le exigen al ciudadano medio, indicando que el sujeto debió haberse comunicado con el servicio de atención general de clientes y, por ende, al sufrir un "engaño" que los magistrados califican como burdo, la entidad bancaria no debía indemnizarlo con el cobro de los seguros asociados al fraude. Sentencia Corte de Apelaciones de Puerto Montt, 3 de agosto 2011, rol Nº 35-2011.

ataques contra intereses o derechos constitucionales cuya protección penal es incuestionablemente necesaria[5].

Así las cosas, de lo que se trata es de, por una parte, reconocer y ponderar las indudables ventajas que tiene para las personas el uso masivo de la tecnología, en una sociedad que ya no concibe su existencia sin ella y, por otra parte, evaluar la necesidad de establecer unos límites precisos, a fin de que ese intercambio de información no amenace con socavar el mantenimiento de las condiciones mínimas que posibilitan la autorrealización individual[6]. En este escenario, resulta fundamental conferir seguridad a los datos personales alojados tanto en redes sociales virtuales como en cuentas de correo electrónico, en la medida en que pueden otorgar antecedentes a terceros para el acceso no autorizado a cuentas bancarias y comerciales, que se han vuelto especialmente vulnerables debido a la masificación de Internet[7].

---

[5] Así, por ejemplo, en un contexto más amplio, los ataques a bienes jurídicos individuales a través de Internet han venido a tener un especial tratamiento en España con ocasión de la Ley Orgánica 5/2010, en vigor desde el 23 de diciembre de 2010, en particular, mediante la inclusión expresa de formas de acoso laboral ("mobbing"), al ciberacoso sexual a menores a través de Internet ("grooming") y el intrusismo informático (hacking), todas cuestiones que se entienden supeditadas a la protección positiva por parte del Código Penal de los derechos constitucionales de integridad moral e intimidad. Un resumen en esta línea, sobre el "bullying" y el "hacking", en la actual regulación española, puede encontrarse en Argenti, Thais - Peleteiro, Almudena, *Luces y sombras de dos de los nuevos delitos introducidos con la reforma penal de 2010*: *el acoso laboral* (*mobbing*) *y el intrusismo informático*, en *Actualidad Jurídica*, 29 (2011), pp. 28 ss. Para una valoración crítica sobre el acoso sexual a menores utilizando Internet, Orts Berenguer, *Delitos contra la libertad e indemnidad sexuales* (*II*), en Vives Antón, Tomás Salvador, *Derecho penal*. *Parte especial* (3ª edición, Valencia, Tirant lo Blanch, 2010), pp. 269 ss. Quintero Olivares, Gonzalo - Carbonell Mateu, Juan Carlos y otros, *Esquemas de la Parte especial del Derecho Penal* (*I*) (Valencia, Tirant lo Blanch, 2011), pp. 146 ss.; González Cussac, José Luis - Matallín Evangelio, Ángela y otros, *Esquemas de Derecho penal*. *Parte especial* (2ª edición, Valencia, Tirant lo Blanch, 2011), pp. 83 ss. En la doctrina nacional, una visión opuesta a la actual tendencia política criminal aquí esbozada puede verse en Escalona Vásquez, Eduardo, *El hacking no es* (*ni puede ser*) *delito*, en *Revista Chilena de Derecho Informático*, 4 (2004), pp. 149-151 y pp. 154 ss. Para una aproximación dogmática al ciberacoso sexual a menores, únicamente: Scheechler, Christian, *El "childgrooming" en la legislación penal chilena*: *sobre los cambios al artículo 366 quáter del Código penal introducidos por la Ley N º 20.256*, en *Revista Chilena de Derecho y Ciencia Política*, 3 (2012) 1, pp. 61 ss.

[6] Véase: Pardo Albiach, Juan, *Ciberacoso*: "*cyberbullying*", "*grooming*", *redes sociales y otros peligros*, en González, Javier (coordinador), en *Ciberacoso*: *la tutela penal de la intimidad*, *la integridad y la libertad sexual en Internet* (Valencia, Tirant lo Blanch, 2010), pp. 54 ss.

[7] En detalle sobre las decisiones jurídicas internacionales de la ONU, OCDE y el

Las páginas que siguen están dedicadas al tratamiento de la significación jurídico-penal del "phishing", del "pharming" y, en menor medida, del "money-mules" en cuanto formas de realización y de participación en la estafa informática, ya calificadas como clásicas modalidades de fraude bancario en el Derecho comparado[8]; sin embargo, en nuestro ámbito no han merecido aún un tratamiento doctrinal extenso y, por ende, se pretende contribuir, en la medida de nuestras limitaciones, al debate sobre las posibilidades y necesidades actuales de incriminación en la ley penal chilena.

II. "Phishing", "pharming" y "money-mules"

El "phishing" y el "pharming" son dos tipos de fraudes informáticos que han aparecido desde mediados de la década pasada[9], cuya finalidad común es la de apoderarse de información personal de un usuario de Internet, para acceder a sus cuentas de correo o de redes sociales y obtener adicionalmente datos de sus contactos virtuales, a fin de comerciarlos ilícitamente, o bien, conseguir claves de "e-banking" para de este modo ingresar a las cuentas corrientes bancarias de los titulares y disponer del dinero que en ellas se encuentra, realizando una operación de transferencia de activos a un tercero que se denomina "mule" (en adelante, mulero o mula). Tal como puede inferirse, el propósito de ambos comportamientos es variado, porque puede ir desde el tráfico de la información obtenida para que terceros interesados en ella realicen envíos masivos de "spam" o correo no deseado, con fines meramente publicitarios[10], pasando por el denominado "malware" o "software malicioso", destinado a infectar los computadores, introduciéndose en el

---

Consejo de Europa, Sieber, *El control*, cit. (n. 1), pp. 173-195.

[8] Así, por ejemplo, en España se califican como las manifestaciones primarias de los fraudes bancarios cometidos por Internet, González Cussac, *Tecnocrimen*, cit. (n. 1), p. 216. Destacando, de modo introductorio al "phishing", que ya es todo un clásico que a las personas se les pidan datos bancarios a través de plataformas informáticas y que paguen por bienes y servicios que nunca reciben, en relación con la regulación alemana, Herzog, Felix, *Straftaten im Internet*, *Computerkriminalität und die Cybercrime Conventio*, en *Política Criminal*, 8 (2009) 4, p. 479.

[9] Ampliamente, en relación con las medidas adoptadas desde los casos que aparecieron en el año 2005 en Europa, Cajani, Francesco, *International* "phishing" *gangs and operation phish & chip*, en *Digital Evidence and Electronic Signature Law Review*, 6 (2009), pp. 153-157.

[10] La finalidad de esta conducta es la utilización del correo electrónico para el envío de publicidad no solicitada, donde el "phishing" y el "pharming" permiten a los creadores del "spam" la indagación de los hábitos de consumo o intereses personales del usuario, creando con ello perfiles para la remisión masiva de información de productos de mercado, aunque la técnica más masificada para ello es todavía el uso de *malware*, generalmente, *cookies* o troyanos en las páginas "web". Vásquez Ruano, Trinidad,

sistema operativo o en el disco duro del equipo, para reconducir a un servidor toda la información que se encuentra alojada o se intercambia por el usuario Internet. Pese a que tales comportamientos valorados en toda su dimensión resultan de gran interés dogmático, acá los tomamos en consideración en cuanto pueden constituir medios para la realización de formas elaboradas o complejas de estafas informáticas, cuyo elemento característico y a la vez diferenciador de otras defraudaciones es utilizar Internet como plataforma de soporte operativo[11].

De entrada resulta de utilidad para fines explicativos, establecer desde ya que la diferencia entre ambas conductas se encuentra más que en los fines en los medios utilizados para obtener los datos. En efecto, mientras en el "phishing" no se utiliza otra cosa que el correo electrónico como soporte material para reconducir a la víctima a un sitio "web" falso[12], en el "pharming" lo que se introduce es un *malware* o un gusano en el servidor de Internet del usuario para reconducirlo mediante la manipulación del "Domain Name Server" (DNS) a una página "web" falsa[13].

Así, una vez que hemos efectuado tales precisiones, podríamos decir que

---

Aproximación jurídica al spam desde la protección de datos de carácter personal, en *Revista de Contratación Electrónica*, 33 (2002), pp. 3 ss.

[11] El "malware" es una expresión ambigua que incluye una amplia lista de programas maliciosos que tienen objetivos variados, que van desde la destrucción de datos alojados en servidores o computadoras personales, pasando por la mera demostración de la vulnerabilidad de los sistemas, hasta el desvío de los servidores DNS con el objeto de redirigir la navegación para la propagación de publicidad, o bien, para introducirse en sistemas de información, a través de la utilización o simulación de datos reales a fin de hacer creer a la víctima que se está contactando con un usuario real, por ejemplo, una página de una entidad bancaria por Internet u otro servicio de carácter comercial. Pardo Albiach, *Ciberacoso*, cit. (n. 6), pp. 66 ss.

[12] Al menos es la variante más conocida, la cual se ha denominado "spear phishing" (pesca con lanza). Acá sólo analizamos esta conducta en la medida en que puede constituir una forma de "engaño", pero puede dar origen a una compleja serie de comportamientos como, por ejemplo, crear cuentas en redes sociales con los datos, atentar contra la intimidad que supone el uso privado el correo electrónico, o bien, incluso, la posibilidad de que con esos datos puedan realizarse transacciones de tipo económico no necesariamente ligadas a la cuenta corriente como tendría lugar con la solicitud de crédito con datos falsos: Mata y Martín, Ricardo, *Estafa convencional, estafa informática y robo en el ámbito de los medios electrónicos de pago. El uso fraudulento de tarjetas y otros instrumentos de pago* (Pamplona, Thomson Aranzadi, 2007), p. 85.

[13] Los servidores DNS están destinados a conducir a los usuarios a la página que desean ver, cuestión que se ve alterada porque el defraudador mediante una manipulación del sistema consigue redireccionar la navegación para que "las páginas visitadas no se correspondan con las auténticas, sino con otras creadas para recabar datos confidenciales": Fernández Teruelo, Javier, *Cibercrimen: los delitos cometidos a través de Internet* (Madrid, Constitutio Criminalis Carolina, 2007), p. 30.

el "phishing" es la pesca de datos personales a través de Internet. Ahora bien, ella puede constituir una modalidad de estafa informática, si tiene lugar a través del envío masivo de correos electrónicos con enlaces a páginas "web" falsas, respecto de las cuales se imita el contenido o la imagen de un determinada entidad financiera o bancaria para engañar al destinatario del mensaje, logrando así sustraer la información personal que posibilita el acceso a sus cuentas de débito personal. De este modo, se logra la consumación de un perjuicio patrimonial mediante el retiro de dinero, o bien, directamente a través de operaciones de compras no consentidas por Internet[14].

A su turno, el "pharming" consiste, según se ha esbozado, en la manipulación técnica de las direcciones DNS que son utilizadas por un determinado usuario, reconduciendo la navegación que este realiza a sitios "web" que presentan un aspecto idéntico, pero que son falsos y han sido creados "con fines defraudatorios". Esta figura puede operar como modalidad de estafa informática si con el mecanismo indicado se consigue la cesión de datos personales financieros o bancarios, con el propósito ulterior de realización de ilícitos de apoderamiento patrimonial de dinero o activos en cuentas corrientes[15].

Finalmente, con los anglicismos "money-mules", "phishing-mules" o "pharming-mules", se hace referencia a una conducta de colaboración que opera con posterioridad a la consumación de la defraudación patrimonial. Ella consiste, esencialmente, en poner a disposición de los estafadores ("scammers") los dineros obtenidos por éstos a través del "phishing" o "pharming"[16].

---

[14] Ampliamente: Velasco Núñez, Eloy, *Fraudes informáticos en red*: *del* "phishing" *al* "pharming", en *La Ley Penal*, 37 (2007), pp. 57-60; Velasco Núñez, Eloy, *Estafa informática y banda organizada*. "phishing", "pharming", "*smishing*" *y muleros*, en *La Ley Penal*, 49 (2008), pp. 19-23; Herzog, Félix, *Straftaten*, cit. (n. 8), p. 480. Un concepto similar sería el de una "práctica en la que el delincuente a través de correo electrónico intenta persuadir al receptor para entregar sus claves personales de acceso a los servicios de banca online": Seidl, Alexander - Fuchs, Katharina, *Die Strafbarkeit des* "phishing" *nach Inkrafttreten des 41. Strafrechtsänderungsgesetzes*, en *Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht*, 2 (2010), p. 85.

[15] Véase, las reseñas a la jurisprudencia española donde se detalla el *modus operandi* de lo que conforme al artículo 242.2 del *Código Penal* español, se entienden mayoritariamente como formas de estafa, Flores Prada, Ignacio, *Criminalidad informática*. *Aspectos sustantivos y procesales* (Valencia, Tirant lo Blanch, 2012), pp. 210-221. También, con referencias a supuestos prácticos, Flores Mendoza, Fátima, *Nuevas modalidades de fraude a la banca electrónica*, en *Nuevos instrumentos jurídicos contra la delincuencia económica y tecnológica*Granada, Comares, 2012), pp. 203 ss.

[16] Conforme a lo expuesto, entendemos que el Ministerio Público incurre en un error conceptual y terminológico al subsumir todas estas conductas en la idea de "phishing", pretendiendo así fundamentar la incriminación de hechos que son claramente diferenciables, recurriendo a generalizaciones que resultan difícilmente aceptables des-

Generalmente, la mula informática pacta con los estafadores una comisión que asciende a la décima parte de las transferencias de origen ilícito[17]. Así, una vez que ha operado el acuerdo y se ha consumado la defraudación, procede al giro de los dineros depositados por los estafadores o "scammers" en sus cuentas de los muleros, que sirven como blanqueadores o lavadores de los montos defraudados en el territorio nacional, en cuanto realizan, posteriormente, las remesas de dichos fondos al extranjero utilizando para ello las casas de cambio establecidas, empresas de paquetería postal y las que ofrecen envíos de dineros al exterior[18].

---

de el punto de vista del contenido de injusto típico. En efecto, entiende que el "phishing" es "un correo electrónico que contiene un link direccionando a una página (falsa) del banco, en la cual le solicitan al cliente sus claves", afirmando que el "pharming" tiene lugar "cada vez que el usuario utiliza su navegador para visitar la página "web" de su banco, se activa un virus informático que recoge y envía información del cliente a terceros". Ambas conceptualizaciones no se corresponden con la dogmática que hay detrás de cada una de estas modalidades de fraudes bancarios, según hemos expuesto. Véase el *Manual para la investigación de fraudes informáticos*. *Unidad especializada en lavado de dinero*, *delitos económicos y crimen organizado de la Fiscalía Nacional* Santiago, Ministerio Público, 2011), p. 4. Este error probablemente esté motivado en un artículo anterior aparecido en la revista institucional, en el que un profesional asesor de la referida unidad, reproduce similares conceptos sin fuentes verificables. Rosenbult Gorodinsky, Verónica, *Punibilidad y tratamiento jurisprudencia de las conductas de "phishing" y fraude informático*, en *Revista Jurídica del Ministerio Público*, 35 (2008), pp. 254-255.

[17] Esta es la constante en España. Así, por ejemplo, la Sentencia del Tribunal Supremo, 20 de marzo de 2013, Nº 227/2013. Antes la Sentencia del Tribunal Supremo, 16 de marzo 2009, Nº 556/2009. En el mismo sentido, la Sentencia de la Audiencia Provincial de Madrid, 7 de Julio de 2009, Nº 355/2009, condena a un sujeto que había reconocido la apertura de una cuenta corriente para el ingreso de cantidades de las que desconoce su procedencia, cobrando por ello un 10% por transferir estas cantidades a un titular que también desconoce a la ciudad de Tallin, Estonia, como autor penalmente responsable de un delito continuado de estafa informática de los arts. 248.2, 249 y 74.2 del *Código Penal*. También, la Sentencia de la Audiencia Provincial de Madrid, 08 de septiembre 2009, Nº 386/2009, aprecia delito continuado de estafa, además condena por asociación ilícita en el caso de un grupo de ciudadanos rumanos que, movidos por un ánimo de lucro, crearon una página "web" fraudulenta, replica de las que permiten el acceso a la banca "online" de determinadas entidades financieras, centrando su actividad en la obtención de datos de usuario, contraseña y coordenadas de seguridad de usuarios de banca online para acceder a cuentas y transferir dinero a otras controladas por la red de crimen organizado.

[18] Se debe tener presente la posibilidad de estar frente a un error, porque muchas veces estas personas son reclutadas a través de ofertas de trabajo falsas y engañosas, en las que se les pide completen un formulario con sus datos personales para ser ingresados en la base de datos de una supuesta empresa oferente. Posteriormente, se les llama por teléfono, o bien, se les contacta a través de Internet, pidiéndole que realicen encuestas y

III. Interrogantes esenciales: una aproximación a las múltiples posibilidades de imputación

Una vez conceptualizadas las conductas que son objeto de estudio y, por ende, trazados unos límites que constituyen lo que podríamos denominar el contenido material mínimo para el establecimiento de un posterior juicio de valoración-atribución de tipicidad de esos comportamientos resulta sumamente útil, incluso con fines didácticos, realizar una aproximación desde lo que ocurre en nuestra *praxis*. De esta forma, podremos tener una idea de la importancia que tiene lo que aquí se aborda y, también, ofrecer una imagen, al menos preliminar, sobre cuál o cuáles podrían ser los títulos de imputación penal.

1. *¿Estafa en concurso ideal heterogéneo con el delito de espionaje informático?*

En el año 2008, el Juzgado de Garantía de Collipulli[19] pronunció una sentencia en juicio abreviado en la cual se enjuició a dos sujetos que habían sido contactados desde México a través de Internet por una persona cuyo nombre virtual era "Jack", a fin de que realizaran una serie de conductas que podríamos resumir en una serie sucesiva de acontecimientos consistentes: primero, en apuntar unos datos personales sobre números de usuarios y claves de accesos virtuales a diversas cuentas corrientes de terceros; segundo, en utilizar esos datos para ingresar por Internet a cuentas corrientes bancarias; tercero, una vez que hubieren logrado acceder a la cuenta debían transferir electrónicamente la totalidad de los fondos que se encontraran disponibles a sus propias cuentas corrientes o a la vista; y, cuarto, realizada esta operación, los sujetos debían retirar los dineros y concurrir a una oficina de transferencia internacional de dinero, en concreto, Western Union y desde ahí remesar a "Jack" las cantidades, pero reteniendo a título de comisión un porcentaje que ascendía a la suma de quinientos mil pesos. En su considerando séptimo la sentencia razona sobre la calificación jurídico-penal de los referidos hechos del modo que sigue: "*Que, los hechos fijados en el razonamiento quinto, configuran el delito del artículo 467 Nº 1º del Código Penal en relación con el artículo 4 de la Ley Nº 19.223, en los que a los acusados les cabe una responsabilidad en calidad de autores, toda vez que, como lo señala dicha norma legal,*

---

efectúen las citadas operaciones de reenvío de dinero reservándose una comisión. Con desglose de casos, Fernández Teruelo, *Cibercrimen*, cit. (n. 13), p. 31; Velasco Núñez, *Estafa informática*, cit. (n.14), pp. 22 ss.

[19] Una reseña de casos a los que resultan aplicables las conclusiones a las que aquí se arriban, puede verse en Rosenbult Gorodinsky, *Punibilidad*, cit. (n.16), pp. 261-263.

en primera instancia existiendo dolo directo de los acusados al desviar dineros de cuentas corrientes pertenecientes a la víctima utilizando medios tecnológicos, es decir, difundiendo la información contenida en dichos medios y luego de ello depositándolos en la cuenta corriente de uno de los acusados, por lo que todos los acusados tuvieron una participación directa en la comisión del hecho ilícito, de conformidad al artículo 15 del Código Penal, hecho que está consumado conforme al artículo 7 del mismo cuerpo legal"[20].

Así las cosas, para el sentenciador los hechos constituyen un delito de estafa y otro de delito de revelación o difusión maliciosa de datos contenidos en sistema de información del artículo 4 de la Ley Nº 19.223, esto es, una modalidad de espionaje informático[21] que, junto al fraude, configurarían una sola acción que al afectar a bienes jurídicos diversos comportaría un concurso ideal impropio en aplicación del artículo 75 CPen., respondiendo todos los acusados son autores. Al respecto surgen, casi de modo inmediato, profundos cuestionamientos a la calificación jurídico-penal que se hace de estos hechos. En efecto, en puridad conceptual, aparece de manifiesto el déficit de fundamentación porque la sentencia no se hace cargo de las razones por las que considera concurrentes los elementos de la estafa. Incluso, hace exclusiva referencia al artículo 471 Nº 1 CPen. que regula la entrega fraudulenta, en cuanto modalidad de la estafa, lo que supone necesariamente la existencia de un título civil obligatorio que ligue a los intervinientes de modo previo, que obligue a cumplir con una entrega que se realiza de modo fraudulento, provocando un perjuicio patrimonial para el sujeto pasivo[22]. Lógicamente, que en la conducta de "phishing" y de "phishing-mules" que efectuaron en tiempos diferentes los sentenciados no hay ninguna obligación civil previa, en consecuencia, aparece manifiesta la citada falta de fundamentación de la que no toca hacerse cargo aquí, por ende, por defecto, asumimos que hace mención a la norma del 467 Nº 1 CPen. para efectos de determinar la penalidad del delito de estafa en relación con la cuantía de lo defraudado.

Entonces, inferimos de la acusación del Ministerio Público que el sentenciador ha querido imputar algunas de los dos formas residuales o básicas de estafa de los artículos 468 ó 473 CPen.[23]. En este orden, la pregunta es si

---

[20] Sentencia Juzgado de Garantía de Collipulli, 10 de marzo 2008, rol Nº 796-2007.

[21] Sobre el contenido de injusto de estos delitos: Huerta, Marcelo - Líbano, Claudio, *Delitos informáticos* (2ª edición, Santiago, Jurídica ConoSur, 1999), pp. 297 ss.; Magliona Markovicth, Claudio - López Medel, Macarena, *Delincuencia y fraude informático*. *Derecho comparado y Ley Nº 19.223* (Santiago, Editorial Jurídica de Chile, 1999), pp. 169 ss.

[22] Véase, por ejemplo, Garrido Montt, Mario, *Derecho Penal*. *Parte especial* (4ª edición, Santiago, Editorial Jurídica de Chile, 2008) IV, pp. 357-358.

[23] Véase, más abajo, la nota 45.

el "phishing" y "phishing-mules" pueden ser consideradas conductas subsumibles en la estafa residual o básica de nuestro *Código Penal* y, también, si el "phishing-mules" es o no una forma de coautoría, o bien, de participación en ese tipo de estafa. La primera pregunta, depende de la respuesta que se dé a un interrogante más general, que dice relación con la posibilidad de imputar penalmente la estafa informática en Chile –posición sostenida entre nosotros por Balmaceda Hoyos[24]– y, al mismo tiempo, qué modalidad de estafa informática es el "phishing". La segunda pregunta, está condicionada por la respuesta de la primera interrogante, pero suponiendo que es afirmativa, lo que habría que plantearse es si un acto de colaboración que tiene lugar con posterioridad al momento en que ha operado la disposición patrimonial puede o no ser constitutivo de coautoría, o bien, se trata de una mera conducta de participación e incluso un delito autónomo[25].

---

[24] Indica que no ve problema alguno para calificar un ilícito como estafa informática en Chile, porque en su opinión el *Código Penal* "sigue -arts. 468 y 473- el sistema ejemplificativo francés, que no contiene una definición general del delito de estafa. Por ello, al contenerse voces como ′el que defraudare a otro′, no vemos ninguna exigencia legal que nos obligue a interpretar al error como elemento autónomo. Así las cosas, y siendo coherentes con su propio sistema (que da una serie de ridículos y trasnochados ejemplos), el delito de estafa informática es punible en Chile, y debe acabarse con la interpretación forzada que de la letra de la ley efectúan la mayoría de la doctrina y jurisprudencia": Balmaceda Hoyos, Gustavo, *El delito de estafa informática* Santiago, Ediciones Jurídicas de Santiago, 2009), p. 121. Entienden que es posible incriminar la estafa informática en el artículo 473 desde la reinterpretación de los elementos "engaño" y "disposición patrimonial": Politoff, Sergio - Matus, Jean Pierre - Ramírez, María Cecilia, *Lecciones de Derecho penal*. *Parte especial* (2ª edición, Santiago, Editorial Jurídica de Chile, 2004), p. 417. También, aunque sin desarrollar nada al respecto, en la medida en que dentro del artículo 473 fuera posible al ser un "tipo de medios abiertos", incluye ahora la denominada estafa cometida a través de medios informáticos: Silva, Hernán, *Las estafas*: *doctrina*, *jurisprudencia y derecho comparado* (2ª edición, Editorial Jurídica de Chile, Santiago, 2005), pp. 29, 108-109. Otra tesis, que compartimos, es que en las manipulaciones informáticas de contenido patrimonial no es posible la incriminación a título de estafa porque la disposición patrimonial la realizan los imputados y no quien es engañado. Implícitamente, Hernández, Héctor, *Perspectivas del Derecho Penal económico en Chile*, en *Persona y Sociedad*, 19 (2005) 1, p. 123. También, pero sólo en el sentido de que reclama la necesidad de una tipificación expresa, igual que lo hacemos nosotros: Mera Figueroa, Jorge, *Delitos contra la propiedad revisión crítica y propuestas de reforma*, en *Revista de Estudios de la Justicia*, 13 (2010), p. 55.

[25] Este problema es relevante por el hecho de que la mayoría de los enjuiciados a título de estafa en nuestro país son personas respecto de las cuales hay dudas que sean directamente quienes "engañan" a las víctimas a través de "phishing" y "pharming", más bien se trata de sujetos que intervienen después que los "estafadores" se han apoderado ilegalmente de las claves y han ingresado al sistema bancario. En consecuencia, no defraudan sino que facilitan sus cuentas corrientes para el traspaso de los activos patri-

2. *Difusión de datos de sistemas informáticos*.

Por el momento, si se nos permite dejar lo anterior pendiente, nos haremos cargo de la segunda imputación, esto es, la estimación de los hechos descritos como constitutivos de la conducta de difusión maliciosa de datos contenidos en sistema de información (artículo 4 de la Ley Nº 19.223)[26]. Al respecto, con la finalidad de pronunciarnos sobre dicha calificación jurídica, deberíamos establecer algunos mínimos conceptuales previos, en concreto, qué puede entenderse, por un lado, por sistema de información y, por el otro, qué es un dato del sistema. A falta de definición legal y escaso tratamiento doctrinal, podríamos recurrir en una interpretación amplia en el contexto de los marcos conceptuales contenidos en la Decisión Marco del Consejo de Europa 2005/222/AI de 24 de febrero de 2005[27]. En este texto se señala que un dato es "*toda representación de hechos, informaciones o conceptos de una forma que permite su tratamiento por un sistema de información, incluidos los programas que sirven para hacer que dicho sistema de información realice una función*"[28]. A su turno, un programa informático es un conjunto

---

moniales a cambio de una comisión por el envío de dinero al extranjero. Pese a ello, incluso considerando la posibilidad que la estafa informática sea punible resulta más que dudoso que pueda considerárseles autores de estafa, ya sea del artículo 15 Nº 1º, o bien, que se estime que su intervención merece la calificación de coautoría o de complicidad elevada a la categoría de coautoría del artículo 15 Nº 3º; es que la sorpresa se incrementa cuando se ve que la calificación jurídica repetida es la de un fraude calificado del artículo 468 CPen. Es más, todo lo anterior tiene lugar en un contexto de "lucha contra el crimen" que raya en la ilegalidad de la investigación, en la medida en que muchas veces son los policías quienes contactan a estos muleros para ofrecerles la referida comisión por el traspaso de activos a sus cuentas personales o por el cobro de vales vistas a su nombre, siendo los agentes policiales los que tienen el contacto con los estafadores que se encuentran fuera del país. Esto puede observarse en la Sentencia del Octavo Juzgado de Garantía de Santiago, 26 de diciembre 2007, autos rol Nº 1745-2007.

[26] El precepto establece lo siguiente: "*El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado*".

[27] Consejo de Europa, Decisión Marco 2005/222/AI de 24 de febrero de 2005 [visible en Internet: http://goo.gl/3QNdd].

[28] Véase el artículo 1 b) de la referida Decisión Marco del Consejo de Europa, cit. (n. 27), pp. 2 ss. Este término, ha sido entendido por nuestra doctrina curiosamente como un concepto no técnico, sino que en el sentido natural y obvio, lo que resulta no ser apropiado en el estado actual de evolución de la informática. Lo mismo ocurre con la idea de soporte informático o sistema, puesto que nuestra doctrina entiende, a nuestro juicio en una mixtura anacrónica, que con la expresión sistema de tratamiento de la información se incluye tanto el soporte físico ("hardware"), como el soporte lógico ("software"), además, de los ficheros o carpetas electrónicas, cuando en realidad son datos. Así, Magliona - López, *Delincuencia*, cit. (n. 21), p. 145. Con matices,

de órdenes o instrucciones que, asociados a parámetros de lógica, dirigen o guían las operaciones de un sistema de tratamiento de información con fines determinados[29]. Finalmente, un sistema informático es "todo aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por estos últimos para su funcionamiento, utilización, protección y mantenimiento"[30].

Ahora bien, sin pretender realizar una interpretación exhaustiva del delito de difusión maliciosa de datos informáticos, porque ello excedería los límites que disponemos, entendemos que hemos de aproximarnos al menos a tres cuestiones, como pasos previos necesarios para calificar como errónea o acertada la interpretación que de los hechos probados efectúa el fallo en cuestión, tales asuntos serían los siguientes: primero, en el plano objetivo, intentar una respuesta sobre qué se entiende por la acción de difundir y qué la diferencia del revelar "datos de un sistema de información"; segundo, responder la interrogante sobre cuál o cuáles son los bienes jurídicos que aquí se protegen; y, tercero, ya en el plano subjetivo, aparece el problema del dolo y su relación con el término "maliciosamente". La orientación para la respuesta debe ser sin perder el marco conceptual de lo que tratamos de ver, esto es, el problema de determinar si en este tipo penal resulta ser subsumible la acción de ingresar a la página "web" de una entidad bancaria con una clave verdadera obtenida indebidamente, para una vez dentro del sistema perjudicar patrimonialmente transfiriendo el dinero que en ella se encuentra disponible.

En relación al primer punto, entendemos, por un lado, que "difundir" consiste en divulgar por cualquier medio a un número indeterminado de terceros los datos contenidos en el sistema de tratamiento de la información perdiendo su control y, por otro lado, que "revelar" es descubrir haciendo manifiestos datos informáticos que se mantienen en secreto[31].

Destacando el concepto de "hecho representado", contenido en el anteproyecto de ley de delitos informáticos, Huerta - Líbano, *Delitos*, cit. (n. 21), pp. 327.

[29] Ampliamente, Miró Linares, Fernando, *Cibercrímenes económicos y patrimoniales*, en Ortiz Urbina, Iñigo (coordinador), *Memento práctico*: *Penal económico y de la empresa 2011-2012* (Madrid, Francis Lefebvre, 2011), p. 474.

[30] Véase, el artículo 1º a) de la referida Decisión Marco del Consejo de Europa, cit. (n. 27), p. 1.

[31] De la Real Academia Española (22ª edición, Madrid, Espasa Calpe, 2001). Si bien, podría pensarse que el sentido de la ley fue ocupar una terminología laxa, con la finalidad de abarcar la mayor cantidad de casos, ello no es óbice para que aquí compartamos la idea expresada por un sector de la doctrina española en cuanto a que es posible distinguir entre difundir y revelar, entendiendo que el primero de dichos tér-

Para que alguna de las modalidades pueda tener lugar se requiere, necesariamente, el acceso previo al sistema de información, porque de otra forma no es posible dar a conocer a terceros los datos que se mantienen reservados dentro del sistema. Así, aparece de modo inmediato la necesidad de dar respuesta a la pregunta sobre el posible concurso entre este delito y el previsto en el artículo 2 de ley de delitos informáticos que, precisamente, fija la punibilidad del acceso indebido. Lo anterior, procurando no perder de vista el inciso 2º del artículo 4 de la misma ley que establece una pena agravada si el sujeto activo que revela o difunde los datos es quien tiene a cargo el sistema de tratamiento de información.

Pues bien, la regla general debería ser que quien accede al sistema no está autorizado para ello (si se quiere no es titular del deber normativo de protección de los datos contenidos en el sistema de tratamiento de información como, por ejemplo, el programador, el soporte técnico informático, ya sea externo o interno), en este caso, lo que sucederá es que necesariamente junto con el delito de revelación o difusión de datos se cometerá de modo previo el de acceso ilícito al sistema con fines de apoderamiento y uso de la información. Con todo, es lógico que el acceso se consume en la revelación o difusión, porque si bien se trata de acciones espacio temporalmente separadas y guiadas con un contenido de dolo específico intensamente subjetivo y claramente diferenciable, sucede que estamos en presencia de un delito mutilado en dos actos donde necesariamente el acceso indebido al sistema con los fines indicados es necesario para lograr la consumación posterior del delito de revelación o difusión de los datos contenidos en el sistema, por tales razones el legislador castiga con un pena única la revelación o difusión de los datos, pena que coincide es su parte más alta con la contemplada para el acceso ilegítimo al sistema[32].

---

minos tiene un alcance de mayor publicidad, de pérdida del control de la información, permitiendo que sea alcanzada por terceros. Bolea Bardón, Carmen, *Arts. 197-216*, en Corcoy Bidasolo, Mirentxu - Mir Puig, Santiago, *Comentarios al Código Penal. Reforma LO 5/2010* (Valencia, Tirant lo Blanch, 2011), p. 469. Entendiendo la revelación como "descubrir o manifestar secretos" y la difusión como la "propagación de conocimiento", tal como lo hace la Real Academia Española, pero, indicando, que no la divulgación no necesariamente debe ser masiva. Magliona - López, *Delincuencia*, cit. (n. 21), p. 169.

[32] Existirá un solo delito de difusión si se trata de una red cerrada o se realiza desde dentro del sistema de tratamiento de información, por ejemplo, computadores con usuarios con carpetas compartidas de archivos personales. Con todo, parece dudoso que pueda plantearse la tipicidad de la revelación o difusión de imágenes o videos personales captados por estas vías, en especial, por el hecho de que conscientemente se han situado datos o hechos de naturaleza íntima o personal en carpetas compartidas y alojadas en un disco duro. Esto tiene importancia para determinar la tipicidad de la

Por el contrario, si quien revela o difunde los datos contenidos en el sistema es precisamente el titular del deber normativo de protección de los mismos, lo que tendrá lugar es solo la figura agravada del artículo 4 inciso 2º, porque quien tiene acceso lícito o autorizado al sistema no puede ser sujeto activo del delito previsto en el artículo 2 de la misma ley. En efecto, lo que se castiga en la figura agravada es el incumplimiento desleal al deber de protección y reserva de los datos secretos contenidos en el sistema de tratamiento de información[33].

Sobre la segunda cuestión planteada, esto es, el bien jurídico que se protege, ha de indicarse, por un lado, que el legislador con estas figuras, en especial, con la norma del artículo 4º de la ley de delitos informáticos, buscaba sancionar una modalidad de espionaje informático[34], y, por ende, no es una figura que su aspecto material contemple la posibilidad de conceptualización como un delito pluri-ofensivo que permita incluir, por esta vía, otros intereses de naturaleza personal como los datos referidos a la intimidad personal en sentido amplio, o bien, si se quiere aspectos de la esfera de autorrealización individual que las personas desean mantener alejados del conocimiento de terceros (hechos relativos a la vida privada o las relaciones familiares lesivos de la fama, crédito o interés), tampoco, posibilita incriminar el apoderamiento de datos de valor patrimonial contenidos en el sistema de información. Por el contrario, lo que tutelan estas normas no es otra cosa que "la información

---

revelación y difusión de datos contenidos en carpetas personales que son distribuidos masivamente por Internet como consecuencia del resurgimiento de los sistemas de intercambio de datos en redes P2P ("peer to peer"), en especial, desde el cierre de "Megaupload" ocurrido en el año 2012. Entendemos que son conductas diferentes porque lo tutelado no es la intimidad, porque si fuese así el asunto debería resolverse en favor de la absorción de la conducta de revelación o difusión de secretos en el delito de acceso indebido al sistema, pero aún para ello se requeriría que hubiere cierta coherencia legislativa y se considerase más grave la revelación o difusión de datos contenidos en el sistema que el acceso. Sobre, la situación en la técnica legislativa española, ampliamente: Fernández Teruelo, *Cibercrimen*, cit. (n. 13), p. 140; Bolea Bardón, "*Arts.*", cit. (n. 31), p. 31; Morales Prats, Fermín - Morón Lerma, Esther, *De los delitos relativos al mercado y a los consumidores*, en Quintero Olivares, Gonzalo (director) y Morales Prats, Fermín (coordinador), *Comentarios al Código Penal español* (6ª edición, Pamplona, Aranzadi, 2011), II, p. 285.

[33] Huerta - Líbano, *Delitos*, cit. (n. 21), p. 305, entienden que siempre el tipo exige como presupuesto para la realización de la modalidad de revelación la existencia de un único sujeto activo que vendría a ser el operador con derecho de acceso al sistema, sin pronunciarse sobre las posibilidades concursarles ni la inclusión o exclusión de la imputación de la modalidad calificada.

[34] Huerta - Líbano, *Delitos*, cit. (n. 21), p. 296; Magliona - López, *Delincuencia*, cit. (n. 21), pp. 50-52.

sobre la información",[35] atribuyéndole a ello la calidad de bien jurídico, es decir, el conocimiento mismo de los datos que en manos de terceros adquieren potencialidad para afectar la fidelidad, la seguridad y el valor patrimonial del sistema en sí mismo considerado[36].

En el fondo, es una figura penal que por la época en que se estableció, más que buscar la protección penal de datos en sentido amplio, esto es, no sólo aquello referido al propio sistema, sino que también incluso los asociados a intereses pluri-subjetivos como, por ejemplo, la intimidad o el patrimonio del tercero titular de información contenida o alojada en el sistema, lo que pretendía en realidad esta norma era tutelar lo que materialmente existía en los albores de la computación que no era otra cosa que la prohibición de revelación o descubrimiento de algoritmos, códigos-fuentes y códigos-objetivos de programas informáticos que constituyen secretos, comprendidos hasta cierto punto en lo que hoy se conoce como secretos de empresa[37]. De ahí,

---

[35] Rovira del Canto, Enrique, *Delincuencia informática y fraudes informáticos* (Granada, Comares, 2002), pp. 70 y 210 ss.

[36] Pese a algunas opiniones que podrían estimar que este precepto protege los datos personales relativos a la intimidad y el patrimonio, no nos parece que sea la tesis correcta. Ello, porque el legislador ha tenido ya varias ocasiones de tutelar penalmente los datos relativos a la intimidad personal contenidos en sistemas de tratamiento informático. En especial, con motivo de la Ley Nº 19.628 sobre protección de la vida privada, de fecha 28 de agosto de 1999, donde se estimó que la revelación y difusión de datos personales alojados en sistemas informáticos, tanto de la esfera de la intimidad como del patrimonio constituyen un ilícito de naturaleza civil. De este modo, el precepto en comento trata un delito de espionaje en sentido clásico, destinado a la tutela de datos de valor industrial, comercial, militar, etc. Para que la tutela de intereses de naturaleza individual fuere posible sería necesario un tipo penal que expresamente declarara la protección de la intimidad personal y, al mismo tiempo, para que el castigo del apoderamiento de datos personales con ánimo de lucro o con la finalidad de apoderamiento patrimonial (por ejemplo, el apoderamiento indebido del "Pinpass"), sea punible es precisa una legislación que se haga cargo de esta cuestión sin dudas sobre las eventuales vulneraciones al principio de legalidad. A modo de ejemplo, pueden verse los comentarios al contenido del artículo 197 del *Código Penal* español, Fernández Teruelo, *Cibercrimen*, cit. (n. 13), p. 140. Ampliamente, sobre la protección penal de la intimidad en la informática, Mata y Martín, *Estafa*, cit. (n. 12), pp. 125 ss.

[37] Ahora bien, podría haber un concurso real con el delito del artículo 81 de la Ley Nº 17.366 de propiedad intelectual (conforme a la reforma que ha tenido lugar en 2010, con ocasión de la Ley Nº 20.435), en relación con su artículo 3 Nº 6 y, sin perjuicio, de las excepciones que se mencionan en el artículo 71 letra Ñ) del mismo texto legal si, junto con revelar y difundir el secreto, se afecta, además, al titular del "copyright" del "software", mediante el copiado y comercialización del programa, por cuanto se lesionaría el derecho exclusivo sobre el aprovechamiento, paternidad e integridad del código fuente, de los códigos objetos y de los manuales asociados, que constituye el objeto material del delito informático en comento. Ahora bien, a esta idea se

que sea una forma de espionaje en sentido estricto[38] y que, en consecuencia, deba interpretarse como una figura que se acerca más, aunque sin serlo íntegramente, a lo que en el Derecho comparado se entiende como tutela del mercado asociado a sistemas de tratamiento de la información y no una cuestión de protección de intereses personales o individuales[39]. Por último, en el plano subjetivo el tipo exige dolo directo[40] de revelar y difundir esos algoritmos, códigos fuentes y códigos objetos que posibilitan el funcionamiento y ejecución del sistema de tratamiento de información, que constituye su esencia y lo hacen diferenciable respecto de otros programas informáticos, otorgándole al mismo tiempo un valor de mercado[41].

---

le puede objetar con cierta razón el hecho de que la ley no hace expresa referencia a los "secretos de empresa", como sí lo hace, por ejemplo, el artículo 278-1 del *Código Penal* español. Véanse: Martínez-Buján Pérez, Carlos, *Delitos relativos al secreto de empresa* (Valencia, Tirant lo Blanch, 2010), pp. 44 ss.; Gallego Soler, José Ignacio, *Arts. 234-262*, en Corcoy Bidasolo, Mirentxu - Mir Puig, Santiago, *Comentarios al Código Penal. Reforma LO 5/2010* (Valencia, Tirant lo Blanch, 2011), p. 559; Morales Prats - Morón Lerma, *De los delitos*, cit. (n. 32), p. 283. Para la construcción de una protección penal de la propiedad intelectual de software puede verse: Mata y Martín, Ricardo, *Desarrollo tecnológico y legislación penal en defensa de los derecho de los creadores*, en *Nuevos instrumentos jurídicos contra la delincuencia económica y tecnológica* (Granada, Comares, 2012), pp. 113 ss.

[38] En efecto, la motivación del delito de espionaje informático es comercial, industrial o militar. Por ello, se le define como "el conjunto de actividades de obtención no autorizada de datos o información de carácter sensible, esto es confidenciales o secretos, de contenido y valor económico patrimonial", no incluyendo nuestro derecho los supuestos en que tales conductas se realizan con ánimo de lucro o en perjuicio de terceros, como sí lo hacía el artículo 197.2 del *Código Penal* español. Véase: Rovira, *Delincuencia*, cit. (n. 35), p. 210.

[39] Véase el comentario al artículo 278 del *Código Penal* español en Santana Vega, Dulce - Gómez Martín, Víctor, *Arts. 278-289*, en Corcoy Bidasolo, Mirentxu - Mir Puig, Santiago, *Comentarios al Código Penal. Reforma LO 5/2010* (Valencia, Tirant lo Blanch, 2011), pp. 608 y 613 ss.; Morales Prats - Morón Lerma, *De los delitos*, cit. (n. 32), pp. 279 ss.

[40] La Corte Suprema en relación con las figuras contenidas en la ley de delitos informáticos ha indicado que la voz "maliciosamente" aquí: "hace referencia a la exigencia de dolo directo, que debe concurrir en el sujeto activo de la conducta, excluyendo toda posibilidad de que pueda cometerse con culpa o dolo eventual, y aquí está claro que el encartado realizó las conductas con pleno conocimiento de los aspectos objetivos y con voluntad de realización" (Sentencia de la Corte Suprema, 2 de abril 2009, rol Nº 4245-08).

[41] Todavía en el supuesto en que se estimase que además este delito protege la intimidad de las personas, la conducta de "phishing" resultaría igualmente atípica en el plano subjetivo porque faltaría el dolo directo (que es el contenido que le damos al término "maliciosamente") de lesionar la intimidad mediante la difusión de datos de la esfera de la privacidad, porque al estafador informático le guía el propósito defraudar

Ahora bien, sobre la base de lo anteriormente expuesto podemos afirmar que la sentencia indicada realiza una calificación errónea de los hechos. En efecto, lo que aquí ocurre es el apoderamiento de datos personales, pero no a través de la revelación del contenido de un sistema informático, ni mucho menos mediante la difusión a terceros de la información contenida en el sistema porque ella no se ha originado en el acceso ilegítimo previo al sistema de tratamiento de datos; por el contrario, ha tenido lugar a través de una manipulación desde fuera del sistema para inducir a error a un sujeto en la medida que voluntariamente ejecuta actos que normalmente no realizaría, que consienten en la entrega de datos personales relativos al acceso a sistemas bancarios[42]. De este modo, si de descubrimiento o revelación de datos puede hablarse, estos tienen lugar no a través del ingreso al sistema, ni tampoco, mediante el quebrantamiento del secreto por parte de usuarios autorizados dentro del sistema, sino que mediante un aprovechamiento de la ignorancia que las personas tienen sobre las medidas de seguridad que se han establecido para resguardar los sistemas bancarios. En puridad conceptual, quien se ha apoderado de las claves de acceso al sistema lo que realiza es una suplantación de la personalidad informática, ingresando al sistema bancario con datos "verdaderos", que no alteran la integridad del "software" informático asociado a la página "web" de la entidad comercial. Estas dos conductas constituyen hechos que merecen ser tratados como delitos independientes y no como meros actos preparatorios de una estafa informática. Ahora bien, como se mencionará (en especial, más abajo III y IV) ninguna de estas conductas resulta ser típica en nuestra legislación[43]. De conformi-

patrimonialmente. Se trata de plus de contenido específico para el dolo directo, que aquí sería el revelar datos con la finalidad de lesionar la esfera de la intimidad pero no el patrimonio. Así, Hernández, Héctor, *Uso indebido de tarjetas falsificadas o sustraídas y de sus claves*, *Política Criminal*, 5 (2008), p. 4.

[42] Fernández Teruelo, *Cibercrimen*, cit. (n. 13), p. 29.

[43] Véase, en del Derecho comparado, en relación con la multiplicidad de ilícitos abarcados. En particular, en la legislación española Velasco Núñez, *Fraudes*, cit. (n. 14), pp. 4-5. En el Derecho Penal francés, junto con discutirse la tipificación de las conductas apuntadas aparece, además, de modo expreso la incriminación del "spam", esto es, el envío masivo de correos electrónicos no solicitados (con ocasión de la Ley Nº 2.004-575 que protege la confianza en la economía digital, de 21 de junio 2004); es una prohibición basada en el principio del respeto al consentimiento expreso del destinatario en la difusión comercial de productos vía Internet. Por este motivo, el *spam* pasó a tipificarse en el artículo 226 Nº 18, inciso 1º del *Code Pénal* francés, sobre lo cualk: Père, David - Forest, David, *L'arsenal répressif du* "phishing", en *Recueil Dalloz* (2006), pp. 2,666 ss. En la legislación alemana, incluso se discute la posibilidad de imputar coacciones en el caso del "phishing" enviado por correo electrónico en el que se dice que en el evento de no darse las claves se procederá al cierre de la cuenta, además, de la posibilidad de sancionar tal como ocurre en España la utilización de programas

dad a lo expuesto, en relación con el fallo que citábamos al principio, como manifestación de la discusión que se da en nuestra praxis sobre este asunto, resulta de evidente que la calificación jurídica de los hechos descritos como difusión o revelación de datos es errónea e incluso antojadiza, en la medida en que la imputación penal que se realiza arroja dudas de adecuación con la prohibición de infracción del principio de legalidad.

3. *¿Ni estafa ni acceso indebido a un sistema informático?*

Otra sentencia pronunciada por un Tribunal Oral en lo Penal[44], sobre la base de un supuesto similar, se hace cargo de enjuiciar a cuatro sujetos, respecto de los siguientes hechos probados que, por su excesiva extensión, siempre procurando mantener el sentido original, ofrecemos en extracto: El día 2 de agosto de 2007, aproximadamente a las 12:41 horas, F.R.G.O. ingresó al sitio "web" del Banco Santander Chile ("office banking"), efectuando una transacción bancaria, por la suma de $15.000.000 de pesos, desde una cuenta corriente ajena cuyo titular es una sociedad comercial a la cuenta corriente de H.A.P. para ello, había obtenido de manera fraudulenta, mediante "phishing", la clave secreta utilizada por la citada empresa para operar por Internet. Ahora bien, para consumar la defraudación F.R.G.O. se contactó con M.E.M.V. a fin de conseguir una persona que mantuviera una cuenta en el Banco Santander Chile, cuenta que debía servir como recipiente del traspaso y retiro inmediato del dinero por caja. Así, M.E.M.V. tomó contacto a su vez con J.R.Z.B. quien se dirigió a H.A.P. cuentacorrentista del Banco Santander Chile, manifestándole que le hiciera el favor de prestar su cuenta corriente para depositar $ 20.000.000, para cumplir un encargo de un primo que vivía en Chiloé, que le había pedido comprar a su nombre dos camionetas en Santiago. Así, H.A.P. accedió a la solicitud como un favor personal, proporcionándole a J.R.Z.B. el número de su cuenta corriente. Realizada la transacción, F.R.G.O. se comunicó con M.E.M.V. y éste a su vez con J.R.Z.B. quien acompañó a H.A.P. a retirar la suma defraudada a la sucursal Huérfanos del Banco Santander Chile, girando el dinero por caja a las 13:31 horas del día 2 de agosto de 2007. Posteriormente, J.R.Z.B. entregó la suma defraudada a M.E.M.V, previa deducción de su comisión ascendente a la suma de $200.000, quien a su vez le entregó, previa deducción de una comisión ascendente a la suma de $ 500.000, el dinero ilícitamente obtenido a F.R.G.O.

El Ministerio Público en su acusación sostuvo, por un parte, que los cuatro

---

destinados a la comisión de delitos de fraude informático, entre otras posibilidades. Seidl - Fuchs, *Die Strafbarkeit*, cit. (n. 14), pp. 86-91.

[44] Sentencia Cuarto Tribunal Oral Penal de Santiago, 13 de enero 2009, rit Nº 131-2008.

acusados tenían participación en calidad de autores de un delito de estafa previsto en el artículo 468 y 467 inciso final CPen.[45], en grado de desarrollo consumado y, por la otra, estimó que G.A.G.S. y F.R.G.O. en concurso ideal

[45] Obsérvese como nuevamente se incurre en el error de estimar que estamos en presencia de un fraude calificado del artículo 468 y no de la figura del artículo 473 CPen. y, además, se les otorga a todos la calidad de autores, incluso a sujetos que realizaron conductas después de configurado el perjuicio (las mulas del dinero), sin distinguir entre los momentos de ejecución ni el grado de participación. Sobre la primera de estas cuestiones, esto es, las razones por la que el Ministerio Público prefiere imputar por estafas calificadas del artículo 468 y no del artículo 473, parecen evidentes desde un punto de vista práctico, pero insostenibles desde una aproximación dogmática. En efecto, la motivación no es otra que la diferencia de penalidad, ya que el artículo 468 lleva asignada una pena mayor que la del artículo 473; sin embargo, el artículo 468 se refiere a las estafas que requieren de una exteriorización, de una puesta en escena constitutiva de engaño bastante y que en un contexto de comunicación pueda inducir a error a otro, es precisa una interacción directa, un acto del lenguaje, una interpretación del sentido de la realidad tergiversada por la distracción que produce el sujeto activo en el intercambio interpersonal directo para llegar a un consenso sobre el contenido de la realidad, de un término o de un concepto, produciéndose de esta forma el error y la disposición patrimonial. Todo ello no se tiene lugar en la estafa informática. La diferencia entre ambos preceptos estimamos se encuentra en que el artículo 473 incluye *algo menos que el ardid y algo más que la simple mentira*. Así: Etcheberry, Alfredo, *Derecho penal*. *Parte especial* (3ª edición, Santiago, 1998), III, pp. 406-407; Grisolía, Francisco, *La estafa procesal en el Derecho penal chileno*, en *Revista Chilena de Derecho*, 24 (1997) 3, pp. 419-420; Silva, *Las estafas*, cit. (n. 24), pp. 29, 108-109; Hernández, Héctor, *La estafa triangular en el Derecho Penal chileno*, *en especial la estafa procesal*, en *Revista de Derecho*, 23 (Valdivia, 2010) 1, p. 221; Yubero, Julio, *El engaño en el delito de estafa*: *doctrina y jurisprudencia* (2ª edición, Santiago, Cruz del Sur, 2010), pp. 104-105; Bullemore, Vivian - Mackinnon, John, *Curso de Derecho penal*. *Parte especial* (2ª edición, Santiago, LexisNexis, 2007), IV, p. 77; Balmaceda, Gustavo, *El delito de estafa*: *doctrina y jurisprudencia* (Santiago, LegalPublishing, 2012), pp. 1 ss.; Fernández Díaz, Álvaro, *Engaño y víctima en la estafa*, en *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, 26 (2005) I, p. 183; Cabrera Guirao, Jorge - Contreras Enos, Marcos, *El engaño típicamente relevante a título de estafa*: *modelos dogmáticos y análisis jurisprudencial* (Santiago, LegalPublishing, 2009), p. 16. Con matices, en la medida que estima que los criterios de diferenciación son ambiguos: Garrido Montt, *Derecho penal*, cit. (n. 22), pp. 368-369. En el mismo sentido, aunque siempre en el entendido de que el artículo 473 sería la figura básica: Piña Rochefort, Juan Ignacio, *Fraude de seguros*, *cuestiones penales y de técnica legislativa* (Santiago, Editorial Jurídica de Chile, 2006), p. 135. Cfr. Politoff - Matus - Ramírez, *Lecciones*, cit. (n. 24), pp. 417-418; Labatut, Gustavo - Zenteno, Julio, *Derecho penal*. *Parte especial* (7ª edición, Santiago, Editorial Jurídica de Chile, 2007), II, pp. 226-227. Aceptando la diferencia, pero no excluyendo la posibilidad de imputar la mentira "contextualizada": Mera Figueroa, *Delitos*, cit. (n. 24), p. 69; Mera Figueroa, Jorge, *Fraude civil y penal*. *El delito de entrega fraudulenta* (Santiago, LexisNexis, 2001), p. 58.

heterogéneo con la estafa, habían consumado en calidad de autores el delito de fraude informático indicado en el artículo 2º de la Ley Nº 19.233[46]. Ahora bien, pese a que el tribunal absolvió de ambas imputaciones por estimar que no se cumplía el estándar de prueba, en cuanto no se acreditaron los hechos, efectúa un análisis de relación entre la estafa informática cometida a través de "phishing" y los elementos de la estafa tradicional y, al mismo tiempo, se pronuncia sobre la calificación jurídica de los hechos como fraude informático.

Pues bien, ahora resulta ser que para los sentenciadores de este caso hechos, idénticos a los de la sentencia anterior, no pueden configuran el delito de estafa, porque los tipos penales del artículo 468 y 473 CPen. requerirían, en todas sus hipótesis, la constatación de la existencia de unos elementos básicos (engaño, error, disposición patrimonial y perjuicio, además de la relación de causalidad entre estos dos elementos), los cuales no se darían en este caso, porque es preciso que el engaño y el error que motiva la disposición patrimonial han de ser provocados y estar dirigidos a una persona física y no recaer en una entidad bancaria. Agrega el fallo que siendo la falsa representación de la realidad por parte del sujeto pasivo lo que le induce a disponer patrimonialmente, no sería posible afirmar que una entidad bancaria en cuanto persona jurídica pueda ser sujeto pasivo de una estafa, al no existir la relación *intuitu personae* exigida por el tipo. En virtud de estos razonamientos, la sentencia afirma categóricamente, en el considerando duodécimo, que no es posible engañar a máquinas, ni sistemas informáticos, porque: "*solo el ser humano puede ser inducido a error, es un fenómeno eminentemente sicológico que hace que la víctima del engaño, indudablemente movida por el error a que ha sido inducida, voluntariamente disponga de los bienes, con perjuicio de su patrimonio o de terceros. Las máquinas no pueden ser engañadas, las máquinas no cometen errores, en consecuencia, solo cabe concluir que el hecho que se ha dejado establecido en la consideración precedente, no es constitutivo de delito, es un hecho atípico, y no puede ser penalmente sancionado, más allá de ser moral y éticamente reprobable*"[47].

Esta es, sin duda, la tesis correcta desde una aproximación tradicional a los elementos del delito de estafa en lo que se refiere al engaño y al error, a los cuales dedicamos, desde nuestra óptica, un apartado especial del presente trabajo (más abajo IV). Si se nos permite, nuevamente, hemos de dejar la cuestión de la estafa para el final y hacernos cargo de la posibilidad de impu-

---

[46] El artículo 2 de la Ley Nº 19.223 sanciona con la pena de presidio menor en su grado medio a "*el que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él*".

[47] Sentencia Cuarto Tribunal Oral Penal de Santiago, 13 de enero 2009, rit Nº 131-2008.

tación penal a título de acceso indebido al sistema, que es la otra imputación que tuvo lugar, a la que dedicamos el siguiente apartado.

4. *Acerca del delito de acceso indebido a sistemas de tratamiento informático.*

En lo que toca al delito informático previsto en el artículo 2 de la Ley Nº 19.223, la Fiscalía imputaba en este mismo caso el acceso a un sistema de tratamiento de información con el ánimo de apoderarse indebidamente de la información contenida en éste. Al respecto, los sentenciadores estimaron que el tipo penal requeriría que el sujeto activo ingresase al sistema informático con la finalidad de utilizar indebidamente los datos, cuestión que no tenía lugar aquí porque el ingreso se habría realizado sin vulnerar o dañar la integridad del sistema por cuanto se usó de una clave verdadera, pero sustraída. Junto con lo anterior, no se denotaba el propósito de usar o apropiarse de la información y, por ende, dado que el tipo penal no protege el patrimonio ni la intimidad personal, sino la integridad de los datos del sistema, el hecho sería atípico[48].

Nada más acertado, porque este tipo penal es una modalidad de espionaje informático que resguarda el secreto o reserva de la información contenida en el sistema de tratamiento de la información, esto es, la incolumidad de los datos cifrados en éste[49]. Efectivamente, pese a que la ley penal utiliza el término "dato", el objeto material está lejos de abarcar la posibilidad de incriminación de la afectación de intereses de naturaleza individual como, por ejemplo, el acceso a un sistema con ánimo de apoderarse de información que pueda poner en peligro o lesionar derechos patrimoniales, derechos de la personalidad, en especial, la intimidad personal o familiar, o bien, el derecho a la propia imagen[50]. Sucede que el tipo penal entró en vigencia antes de la masificación de Internet y de los computadores personales y, por ende, estaba pensando para la realidad de fines de los años ochenta y principios de los noventa del siglo pasado, donde los sistemas de tratamiento de información

---

[48] Sentencia, cit. (n. 47), considerando 12°.

[49] Con matices: Magliona - López, *Delincuencia*, cit. (n. 21), p. 164.

[50] Como tiene lugar, por ejemplo, con el tipo penal del artículo 197 del *Código Penal* español. Véanse: Flores Prada, *Criminalidad*, cit. (n. 15), p. 60 ss.; Morales Prats, Fermín, *Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio*, en Quintero Olivares, Gonzalo (director) - Morales Prats, Fermín (coordinador), *Comentarios al Código Penal español* (6ª edición, Pamplona, Aranzadi, 2011), I, pp. 1.287 ss. En Chile entiende que es posible de *lege data* entender que se protegen dichos bienes, en especial, la intimidad: Jijena Leiva, Renato Javier, *La protección penal de la intimidad y el delito informático* (Santiago, Editorial Jurídica de Chile, Santiago, 1992), p. 31. Otro sector de nuestra doctrina deja abierta tal posibilidad en relación con el tipo penal del artículo 4 de la ley delitos informáticos: Huerta - Líbano, *Delitos*, cit. (n. 21), p. 305.

eran cerrados, en su mayoría insertos en servidores estáticos que alojaban programas adaptados para procesos acotados de producción industrial o pensados para el acopio y sistematización de información en labores gubernamentales o de investigación universitaria, con escasa o nula capacidad de almacenaje de datos dentro del sistema, más allá de los necesarios para posibilitar su funcionamiento[51].

Por si esto fuera poco, no había protección de los programas computacionales a título de propiedad intelectual como existe hoy. Por todas estas cuestiones, el objeto del delito son casi exclusivamente los algoritmos, códigos-fuentes y códigos-objetivos de programas informáticos, incluyendo, los datos que han posibilitado la mejora del sistema de tratamiento de información, datos de investigación, de defensa, de recursos humanos de una empresa o entidad, de contabilidad empresarial, incluidos los datos de clientes, sin que resulte alteración del "hardware"[52] (por ejemplo, a través de la extracción del disco duro, porque ello quedaría dentro del tipo del artículo 1 de la citada ley).

Es un tipo penal totalmente anacrónico, que precisa *de lege data* una modificación en orden a otorgar protección a los datos reservados de carácter personal o familiar que se hallen registrados en ficheros o soportes informáticos, castigando su uso o alteración en perjuicio del titular o de terceros, tal como lo proponía tímidamente el *Anteproyecto de Código Penal* chileno de 2005, en cuanto consagraba una modalidad difusa de atentado a la intimidad en el acceso de la información contenida en sistemas informáticos de tratamiento de información sin la voluntad del titular del soporte (artículo 135.5º)[53].

Ahora bien, en directa referencia a lo que nos ocupa ha de indicarse que el ingreso a un sistema de tratamiento informático usando indebidamente los datos contenidos en éste, con ánimo de lucro y en perjuicio de un tercero, modificando su situación patrimonial, no es punible en nuestro derecho, a menos no a título de este artículo 2 de la ley de delitos informáticos[54]. En su

---

[51] Con amplias referencias relativas al caso de espionaje informático ocurrido en 1988, entre empresas alemanas y francesas para la realización de un tren de alta velocidad en Corea del Sur, donde los agentes comerciales franceses interceptaron la oferta de la alemana Siemens enviada por fax a través de un sistema de tratamiento de datos satelital: Sieber, Ulrich, *Legal Aspects of Computer-Related Crime in the Information Society COMCRIME. Study prepared for the European Commission* (Santa Clara, University of Würzburg, 1998), p. 44 [visible en Internet: http://goo.gl/fDHBL].

[52] Ampliamente, sobre esta realidad: Rovira, *Delincuencia*, cit. (n. 35), p. 211.

[53] AA.VV., *Anteproyecto de Código Penal Chileno de 2005, elaborado por la Comisión Foro Penal*, en *Política Criminal*, 1 (2006), pp. 30-31.

[54] Tanto es así, que conscientes de esta realidad los redactores del Anteproyecto de Código Penal de 2005, propusieron a continuación de la regulación de la estafa, en un parágrafo 8 especialmente dedicado al perjuicio mediante el uso indebido de sistemas

aspecto subjetivo, el delito exige como dolo específico que el sujeto tenga por finalidad el apoderarse, usar o conocer de los datos contenidos en el sistema de tratamiento de información y, por ende, la finalidad de apoderamiento de datos con ánimo de perjudicar patrimonialmente a un sujeto determinado no está abarcado por el tipo penal[55]. En efecto, si alguna reinterpretación en aras de su adecuación a la realidad actual puede hacerse –aunque con bastantes dudas sobre el respeto al principio de legalidad–, partiría por asumir que lo que se penaliza aquí es el acceso ilegitimo con fines de apoderamiento, uso o conocimiento, a servidores gubernamentales o universitarios que pueda poner en peligro las ventajas competitivas en un mercado o área de desarrollo determinada para el caso de los procesos industriales o servicios específicos, o bien, los datos que terceros puedan obtener de clientes, trabajadores o estudiantes (por ejemplo, la dirección, nombre, teléfono y correo electrónico), en cuanto eventualmente puede ser comercializados o cedidos a empresas, políticos o particulares para la difusión de información publicitaria[56], como valores de mercado.

En consideración a lo expuesto y en relación con la conducta objeto de calificación jurídica en el fallo, debe reconocerse de entrada que nuestra ley

---

de información, una norma (artículo 160) que indicaba lo siguiente: "*En las mismas penas del artículo anterior incurrirá el que*, *con ánimo de lucro*, *modifique una situación patrimonial en perjuicio de otro*, *alterando indebidamente el funcionamiento físico o lógico de un sistema de tratamiento automatizado de información o los datos contenidos en el mismo*, *utilizando indebidamente en el mismo datos verdaderos o falsos o valiéndose indebidamente de cualquier otra manipulación o artificio semejante que altere física o lógicamente el funcionamiento del referido sistema*". AA.VV., *Anteproyecto*, cit. (n. 53), p. 35. artículo 160

[55] Hernández, *Uso indebido*, cit. (n. 41), p. 4.

[56] Las dudas se sitúan en la incongruencia de esta posibilidad con el bien jurídico, porque aquí lo tutelado no es la intimidad en su amplia dimensión. La eventualidad de incriminación de tales conductas vendría dada por la aceptación de la concepción de la doble dimensión de la intimidad, según la cual, por un lado, se contiene en ella una vertiente positiva caracterizada por el ejercicio de un poder de control sobre la información y los datos ya conocidos que solo podrían ser utilizados con la autorización de su titular y, por la otra, un contenido negativo, conforme al cual las personas tienen un derecho a excluir del ámbito de la vida privada a los demás, otorgándole a dichos espacios la naturaleza de secretos. Únicamente, esta última dimensión encontraría en nuestro derecho una protección penal, en el artículo 161-A CPen., aunque sin mención de la difusión por medios informáticos de datos como la imagen o los videos alojados en bases de datos privadas. La segunda dimensión, tiene consideración únicamente como daño civil de la difusión de datos personales, sólo podría tener cabida en este artículo 2 de la ley de delitos informáticos, pero con las limitaciones expuestas. Sobre la doble dimensión de la intimidad en relación con la informática, Véase: Muñoz Conde, Francisco, *Derecho penal. Parte especial* (18ª edición, Valencia, Tirant lo Blanch, 2010), pp. 270-271.

no establece la punibilidad del mero ingreso no autorizado a una sistema informático, incluso, no son punibles las conductas posteriores al acceso como, por ejemplo, la permanencia ilícita dentro de un sistema informático de gestión o tratamiento de datos. De este modo, quien ingresa indebidamente por diversión, o bien, para demostrar o probar que el sistema es vulnerable no comete delito alguno, porque el "hacking"[57] no es una conducta punible en Chile[58]. Esta afirmación se desprende de la historia fidedigna del establecimiento de la norma, en particular, de las fuentes que se tuvieron en cuenta para su redacción[59]. Ciertamente, del debate parlamentario[60] se infiere que el legislador se apartó, probablemente por un defecto de técnica, de la legislación francesa de la cual se sirvió en este punto, por cuanto, aquélla sí considera punible el mero acceso, conforme se desprende del actual artículo 323-1, inciso 1º del *Code Pénal* francés de 1992, que corresponde al artículo 462-2 del Código derogado[61].

---

[57] El "hacker" no es más que un curioso informático que ingresa a los sistemas informáticos, sin dañar, alterar o apoderarse de ningún tipo de fichero o dato, a lo más deja unos "logs" necesarios para hacer desaparecer el rastro. En general, son personas que conocen a fondo los lenguajes de programación, los protocolos de Internet (TC/IP) y una multiplicidad de tipos "software" de manejo o soporte de datos. En cuanto a la finalidad de su conducta, ella no es la de vulnerar el sistema, ni apoderarse de los datos, ni perjudicar a terceros, sólo pretende "mirar" u "observar" desde dentro de éste, para así lograr mayores conocimientos y aprendizajes. Este tipo de "hacker" es denominado "blanco" para diferenciarlo de los "crackers" que tienen por objeto vulnerar el sistema, introducir virus, apoderarse o eliminar datos o ficheros. Sobre esto: Morón Lerma, Esther, *Internet y Derecho penal*: "*hacking*" *y otras conductas ilícitas en la red* (Pamplona, Aranzadi, 1999), p. 42 ss.; Monterde Ferrer, Francisco, *Especial consideración de los atentados medios informáticos contra la intimidad y la privacidad*, en *Delitos contra y a través de las nuevas tecnologías ¿Cómo reducir su impunidad? Cuadernos de Derecho Judicial*, 3 (2006), pp. 200 ss.

[58] Así, por ejemplo: Huerta - Líbano, *Delitos*, cit. (n. 21), p. 302; Escalona, *El* "*hacking*", cit. (n. 5), p. 154.

[59] Esta referencia en: Magliona - López, *Delincuencia*, cit. (n. 21), pp. 165-167.

[60] Véase el proyecto y los dos informes de la Comisión de Constitución, Legislación, Justicia y Reglamento en el *Boletín* Nº 412-2007/1991 [visible en Internet: http://goo.gl/JAEK6].

[61] El *Code Pénal* francés de 1992, después de las reformas que han tenido lugar con motivo de la Ley Nº 575-2004, de 21 de enero de 2004, además, de lo previsto con ocasión de la reforma operada con la Ley Nº 410-2012, de 27 de marzo de 2012, establece en el citado artículo 323-1 inciso 1º que castiga con una pena de dos años de prisión al que acceda o permanezca de manera fraudulenta en todo o en parte de un sistema automatizado de datos. Indicando, el inciso 2º, que la pena es de tres años de prisión y una multa de 45.000 euros si el resultado es la supresión o modificación de los datos contenidos en el sistema o problemas de funcionamiento en éste. Finalmente, el inciso 3º consagra una figura calificada, en cuanto dispone que la pena se elevara a cinco

Una mirada comparativa permite constatar las diferencias casi de modo inmediato, ya que la norma francesa no precisa de ningún contenido subjetivo específico adicional al dolo, es suficiente con el conocer que se accede sin autorización al sistema. Por el contrario, el tipo penal del artículo 2 de la ley de delitos informáticos exige que el sujeto activo ingrese indebidamente y, además, lo haga para "usar", "apropiarse" o "conocer", los datos del sistema[62]. Pues bien, sucede que el "phishing" el sujeto lo que hace es ingresar a un sistema de tratamiento de información suplantando la identidad de otra persona que sí está autorizada para el ingreso. En efecto, la entrada se realiza con una clave verdadera, facilitada por el titular de la misma es "indebida" en el sentido de que su uso no ha sido autorizado por éste. Por tales razones, hay que indicar que tampoco se vulneran ni dañan las barreras de seguridad previstas para el correcto funcionamiento e integridad del sistema; es decir, no se ingresa alterando el "software" del portal "web" de la entidad bancaria para así lograr una vía de ingreso distinta de la que se ha destinado por el programador. De ser así, la pregunta es si es o no posible subsumir los actos de obtención y uso ilegítimo en el portal "web" de una entidad bancaria en alguno de los tipos penales existentes.

Al respecto, descartar de entrada la suplantación de la identidad informática, porque no encuentra respuesta penal en nuestro Derecho como sí ocurre en otros ordenamientos, donde la usurpación de nombre es planteada

---

años de prisión y a una multa de 75. 000 euros si los delitos indicados en los incisos anteriores se han cometido en contra de un sistema de tratamiento automatizado de datos personales [visible en Internet: http://goo.gl/AqIPl]. Sobre el régimen general de la estafa en el código francés, véase: Conte, Philippe, *Droit pénal spécial* (3ª edición, Paris, LexisNexis, 2007), pp. 331 ss.

[62] Las acciones típicas por las cuales pueden verse realizadas tales finalidades son la intercepción, interferencia y acceso al sistema. Respecto de las dos primeras debe indicarse que, por una parte, la intercepción consiste en el desvío de la comunicación contenida en el sistema evitando que la misma llegue al destinatario y, por la otra, interferir es perturbar la transferencia normal de datos del sistema. En ambos casos, es preciso que el sujeto realice las citadas conductas con un contenido de dolo específico, o bien, si se quiere conforme a la exigencia de un especial ánimo subjetivo. Es más las conductas de interferencia de comunicaciones como, por ejemplo, el denominado "wardriving", esto es, la conexión a una red "Wi-Fi" ("Wireless Fidelity") ajena sin el consentimiento del titular, utilizando una clave obtenida ilícitamente es impune, incluso si a través de la red se tiene acceso a ficheros o datos contenidos en otros computadores que la utilizan y, lamentablemente, el apoderamiento de imágenes personales, videos o datos contenidos en las carpetas, en cuanto su conocimiento implique afectación de la intimidad, resulta no ser punible en nuestro derecho. Sobre estas conductas, en relación con el artículo 255 del *Código Penal* español, véase: Fernández Teruelo, *Cibercrimen*, cit. (n. 13), pp. 152 ss.

como una salida *de lege data* atendible para estos casos[63]. Es que aunque los tipos sean más o menos coincidentes surgen dudas sobre las posibilidades de incriminación por dicha vía, en especial, porque bajo el amplio concepto de nombre a que hace referencia el tipo penal del artículo 214 CPen., se entiende sólo el verdadero o real, no el seudónimo ni al inventado[64], que se corresponde más con la naturaleza de los nombres hipocorísticos que se usan por los usuarios para identificarse en Internet, al mismo tiempo, tampoco es posible comprender dicha norma con referencia los datos asociados a la identidad que son los que aquí propiamente se usan, por ejemplo, los números de cédula de identidad o de documentos nacionales de identidad de otros países, pasaporte, o bien, claves asociadas a sistemas de tratamientos de datos.

5. *Posibilidades de imputación de la obtención y uso de claves sustraídas.*

Sobre este punto, relativo a la obtención y uso ilegítimo de claves de acceso a sistemas informáticos bancarios vía Internet es preciso realizar una distinción entre, por una parte, las claves asociadas a cuentas bancarias y, por la otra, las claves y números de tarjetas de crédito que son utilizadas como formas de apoderamiento patrimonial, generalmente, a través de compras "online".

En lo que se refiere a las conductas de "phishing" y "pharming" que recaen en la obtención de datos numéricos del titular de una cuenta corriente, incluyendo su identificación y claves, sólo es posible discutir la imputación penal a título de tentativa de estafa. Sin embargo, dada la inexistencia de una tipificación expresa del delito de estafa informática, la correlativa imposibilidad de imputación de la tentativa se hace todavía más evidente. Más aún, tal como ya se ha indicado, no resulta posible recurrir al delito del artículo 2 de la ley de delitos informáticos en el evento de que se obtuvieran las claves o los datos de acceso a sistemas bancarios, mediante el acceso a distancia al sistema operativo de un computador personal conectado a un red local, apoderándose de las carpetas y ficheros, a través de su transferencia o registro mediante copia de toda la información, cuya finalidad es la búsqueda de archivos que contengan información relativa a las claves bancarias. En este caso, ya nos desviamos el "phishing" y el "pharming" toda vez que las

---

[63] Velasco Núñez, *Fraudes*, cit. (n. 14), pp. 59 ss.

[64] Así: Etcheberry, Alfredo, *Derecho penal. Parte especial* (3ª edición, Santiago, Editorial Jurídica de Chile, 1998), IV, p. 201. Por la alternativa de sólo exigir la utilización del uso de una identidad que pueda inducir a error a otra persona física, con lo cual igualmente el hecho resultaría atípico, ya que aquí se induce a error a un soporte informático: Bullemore - Mackinnon, *Curso*, cit. (n. 45), p. 145. Entiende que el nombre de pila y el patronímico deben ser utilizados conjuntamente: Garrido Montt, *Derecho Penal*, cit. (n. 22), p. 147.

modalidades de acceso remoto a un computador personal conectado a una red de Internet a través de "spyware" (por ejemplo, los troyanos y las bombas lógicas, que se descargan por Internet y se instalan con controles "ActiveX", generalmente, desde páginas poco fiables o inseguras, o bien, a través de programas de "freeware" o "shareware") se realizan sin interacción alguna con el titular de la cuenta[65].

Queda hacerse cargo de las conductas que tienen por objeto la obtención de claves y datos personales que recaen en tarjetas de crédito. Ellas podrían constituir, eventualmente, actos preparatorios del delito previsto en la letra d) del artículo 5 de la Ley Nº 20.009, en cuanto allí se sanciona el uso de los datos o del número de la tarjeta de crédito, haciendo posible que terceros realicen operaciones de compra o de acceso al crédito o al débito. Lógicamente, estamos en presencia de una conducta impune, porque en nuestra ley no se castiga la posesión de las claves ni su obtención indebida, únicamente deviene en punible desde que se usa de ella; lo que ya constituye *per se* un adelantamiento de punibilidad en relación con el perjuicio patrimonial.

Ahora bien, es cierto que esta ley hace mención expresa a las tarjetas de débito (artículo 5); pero, la referencia sólo tiene valor en la medida en que éstas sean utilizadas material o físicamente[66]. En efecto, implícitamente adscribe a la idea de uso a través de la realización de giros de dinero desde o a través de cajeros automáticos, o bien, mediante la compra directa en el comercio. No se refiere la ley a las posibilidades de obtención mediante engaño de las claves que posibilitan el acceso a la cuenta bancaria a través de Internet, que son datos que no se encuentran incorporados en la tarjeta de débito física, a diferencia de lo que tiene lugar con la tarjeta de crédito, en cuanto la posesión de los datos contenidos en ella posibilita la compra "online" de activos patrimoniales[67].

Ahora bien, aquí resulta difícil estimar en términos prácticos la posibilidad de participación de la mula de dinero ("money-mules"), puesto que lo habitual, en relación con el uso o utilización de tarjetas de crédito, es que aquí se efectúen compras directas de objetos físicos por Internet. Con todo,

---

[65] Una técnica ya muy expandida es el uso de los denominados "keyloggers" que son programas que registran todo lo que se teclea en el computador, en especial, el registro que se origina a través de la navegación en Internet; véase: Fernández Teruelo, *Cibercrimen*, cit. (n. 13), pp. 28-29.

[66] Es un modelo que se construye sobre la base de la utilización de la tarjeta como objeto]; véase: Hernández, *Uso indebido*, cit. (n. 41), p. 19.

[67] En tal sentido, la citada ley soluciona de un modo bastante práctico la enconada discusión que se dio, por ejemplo, en España en relación a la posibilidad de imputar hurto, robo con fuerza en las cosas o estafa informática. Véase: Azcona Albarrán, Carlos, *Tarjetas de pago y Derecho penal. Un modelo interpretativo del artículo 248.2 c) del Código Penal* (Barcelona, Atelier, 2012), pp. 149 ss.

habría que admitir que los muleros pueden ser utilizados como destinatarios de despachos por correo, es decir, como receptores y remisores posteriores de los bienes adquiridos con las tarjetas de crédito. En este supuesto, estamos en presencia de un acto que ha de ser calificado como posterior a la consumación de la modalidad agravada de perjuicio patrimonial que el mismo artículo 5 en su inciso final de la Ley Nº 20.009 castiga con la exclusión del mínimo de la pena para los autores.

El problema en estos supuestos se reduce en nuestro ordenamiento a la discusión sobre si el mulero realiza una conducta que puede ser calificada como receptación, o bien, como encubrimiento por aprovechamiento (artículo 17 Nº 1 CPen.) del delito contemplado en el citado artículo 5 de la Ley Nº 20.009. En efecto, en el entendido de que el mulero realiza un acto que es siempre posterior a la consumación del perjuicio patrimonial, ha de ser considerado siempre como un participe en relación con el robo o el hurto de la tarjeta de crédito, o bien, como un encubridor del delito previsto en la letra d) del artículo 5º de la Ley Nº 20.009, si la compra se ha realizado por Internet previa obtención mediante "phishing" o "pharming" de los datos que de la tarjeta de crédito son necesarios para efectuar compras "online" (nombre del titular, números de serie, fecha de caducidad y código de seguridad del dorso). Este razonamiento viene justificado, por una parte, por la circunstancia de que el tipo penal de receptación del artículo 456-A CPen. no se refiere a las especies muebles que provienen de fraudes especiales (en este caso los de la Ley Nº 20.009), pero sí hace mención al robo y al hurto y, por otra parte, porque el modus operandi en que tiene lugar la participación de los muleros implica generalmente la exigencia de una comisión por el servicio que prestan; en consecuencia, su actividad se corresponde en este caso con el tipo de encubrimiento por aprovechamiento (artículo 17 Nº 1). Lógicamente, que ello dependerá de la acreditación y prueba que había conocimiento de la procedencia ilícita de las especies, asunto que ofrece incluso más dudas porque se ha constado que las mulas son casos supuestos íconos de ausencia de dolo por instrumentalización[68].

[68] Al respecto, en España recientemente la sentencia de la Audiencia Provincial de Madrid, 29 de julio 2010, Nº 332/2010, absuelve a un acusado por error de tipo vencible (al excluirse la imputación imprudente de estafa informática en el *Código Penal* español), puesto que estimó que en realidad había sido engañado por unos sujetos de Europa del Este que se aprovechan de la situación de vulnerabilidad económica en que se encontraban varias personas, a las que les ofrecieron "teletrabajo" con el atractivo de ganar dinero de manera fácil y rápida desde sus casas contestando encuestas, bajo las condiciones de disponer de una cuenta corriente donde recibir dinero de supuestos "clientes" encuestados y una red de Internet funcionando las veinticuatro horas. Siguiendo las órdenes de las supuestas actividades mercantiles, el acusado giraba los montos depositados, reservándose para sí una cantidad que oscilaba entre el 5% y el

6. *¿Es la clave de acceso a la cuenta corriente una "llave falsa"?*

Una vez que se ha realizado esta aclaración, queda hacerse cargo sobre la eventualidad que el uso de la clave de entrada al sistema bancario facilitada con el consentimiento inválido del titular de la cuenta, además, de las otras claves que posibilitan la transferencia de los activos patrimoniales existentes en la cuenta corriente, como es el caso de las claves de seguridad creadas para transferencia electrónica ("Pinpass"), puedan o no constituir "uso de llaves falsas" en el sentido del delito de robo con fuerza en las cosas. Al respecto, si bien ello podría ser posible en un concepto extensivo de llave falsa como el que contempla, por ejemplo, el artículo 239 del *Código Penal* español[69], en nuestro Derecho a falta de una norma expresa que facilite la asimilación, es podría sostenerse en *strictu sensu* que la clave de acceso al portal "web" de una entidad bancaria es una llave falsa con idéntico contenido conceptual del exigible para configurar el delito de robo con fuerza en las cosas.

En efecto, si bien podría sostenerse que quien hace uso de una clave numérica de acceso a un sistema bancario está utilizando un instrumento tecnológico que sirve para abrir a distancia un "lugar cerrado" y en la medida en que la clave se obtiene con el consentimiento inválido del dueño, surge de inmediato el problema que aquí no estamos en presencia de un lugar físico propiamente tal, en cuanto pueda decirse que la clave sirva para acceder al lugar cerrado en que se encuentra el dinero, o bien, que sea útil para abrir a distancia la caja del banco, puesto que aquí lo que se hace no es otra cosa que activar una plataforma o soporte informático. La imposibilidad de entender esto último como un lugar "físico", porque es obvio que es "virtual", unido al hecho de que la clave se entrega con consentimiento del titular (viciado o en error), excluye toda posibilidad de imputación por este título.

7. *Acerca de la eventualidad de sanción a título de hurto.*

Algo similar ocurre con el hurto donde los problemas de tipicidad objetiva parten desde la consideración de la concurrencia del objeto material; es que resulta complejo afirmar que aquí estamos en presencia de una cosa corporal mueble. En efecto, si bien no hay dudas de que el dinero es un objeto corporal mueble susceptible de apropiación e inherentemente pecuniario sucede

---

10% a título de comisión, enviando el saldo restante a "los empleadores" mediante los servicios de empresas de envío de dinero como Money Gramm o Western Union a Rumanía y Ucrania.

[69] Conforme al artículo 239.3 inciso 2º que establece lo siguiente: "*A los efectos de este artículo, se consideran llaves las tarjetas, magnéticas o perforadas, los mandos o instrumentos de apertura a distancia y cualquier otro instrumento tecnológico de eficacia similar*". Sobre este punto: Azcona Albarrán, *Tarjetas*, cit. (n. 66), p. 109 ss.; Muñoz Conde, *Derecho penal*, cit. (n. 56), p. 396.

que, por un lado, el contrato de cuenta corriente da al librador únicamente el derecho personal de girar o generar órdenes de pago sobre los saldos de dinero depositados en la cuenta o de los créditos que se hubieren estipulado cuyo único dueño es el banco y no el cuentacorrentista[70] y, por otro lado, pasa que aquí en rigor lo que tiene lugar es una alteración del pasivo contable a través de una manipulación fraudulenta de datos informatizados alojados en la banca electrónica realizados con ánimo de enriquecimiento ilícito. Si se tratara de un hurto se requeriría además que existiera una coincidencia entre el momento en que el dinero sale de la esfera del dueño – en este caso del banco– y su aprehensión física corporal por parte del sujeto activo, lo que aquí no tiene lugar porque en realidad lo que ocurre no es otra cosa que una alteración de datos de un sistema informático (que no revisten la naturaleza de cosa corporal mueble), realizada con ánimo de lucro y que se perfecciona en el momento en que ocurre la anotación (que no es más que engañar al sistema para que emita una orden de pago), de las sumas transferidas a la cuenta del autor o de un tercero (la "mula"). En otros términos, se trata de una figura que reviste el *modus operandi* propio de los actos defraudatorios, aunque no en todos los supuestos tenga lugar algún grado de engaño para obtener la clave secreta de acceso a la cuenta corriente[71].

Con todo, las posibilidades van por la vía de considerar que los cuentacorrentistas tienen el derecho a exigir el cumplimiento del deber de custodia, protección o fidelidad por parte de las entidades bancarias a fin de que exista una efectiva administración y resguardo de activos patrimoniales. Probablemente, estas razones llevaron al *Anteproyecto de Código Penal* de 2005 a proponer una figura similar a la que existe en el Derecho alemán, en cuanto pareció estimarse que en estos casos estamos en presencia de un uso no autorizado de datos correctos que se entregan incluso de modo consentido y, por ende, se requeriría de un tipo delictivo que alejándose de la estafa tradicional se emparentara tanto con los delitos informáticos como con el delito de administración desleal; en consecuencia, buscaba incluir los supuestos en que se utilizan o alteran datos informáticos con autorización para manipular el sistema (un dependiente del banco que se apodera desde dentro manipulando los datos de la cuenta corriente), como también, la posibilidad de apoderamientos patrimoniales con datos obtenidos previamente mediante engaño[72].

---

[70] Así: Hernández, *Uso indebido*, cit. (n. 41), p. 13 ss.

[71] Véase: Gutiérrez Francés, María Luz, *Fraude informático y estafa. Aptitud del tipo de estafa en el Derecho español ante las defraudaciones por medios informáticos* (Madrid, Ministerio de Justica Secretaría General Técnica, Centro de Publicaciones, 1991), pp. 589 ss.

[72] Véase el artículo 160 transcrito en la nota 54, AA.VV., *Anteproyecto*, cit. (n. 53),

8. *Delitos relativos a la propiedad industrial asociados al uso de la imagen de la entidad bancaria*.

Otra posibilidad que debe ser descartada aquí antes de entrar al problema de la estafa, es la cuestión relativa al uso de la imagen comercial de una entidad bancaria la que encuentra protección en la ley de propiedad industrial. En efecto, a través del "phishing" y "pharming" se duplica la imagen de una "web" bancaria para hacer creer que quien se comunica con el usuario es el banco. En otros ordenamientos es posible imputar aquí un delito contra la propiedad industrial en concurso medial con la estafa informática[73], pero en nuestro Derecho el tipo penal de la letra b) del artículo 67 de *Ley de propiedad industrial*[74] que se refiere al uso no autorizado de la imagen de una empresa no hace mención a la posibilidad de que el uso se realice con fines ilícitos, ya que se reserva –por defecto de técnica legislativa– para la aplicación del tipo solamente a los supuestos en que se utiliza con fines comerciales, añadiendo un especial *animus* al contenido subjetivo del injusto.

IV. Dificultades para la subsunción del "phishing" y el "pharming" en el modelo tradicional de estafa

En los párrafos anteriores se ha advertido sobre la importancia y actualidad que tienen estos fraudes bancarios y, al mismo tiempo hemos descartado las posibilidades de imputación como delitos informáticos en sentido estricto y, también, se ha hecho referencia a las necesidades de punición que enfrenta nuestro Derecho, en particular, debido a los múltiples intereses que aparecen faltos de una protección penal. Preliminarmente, podemos afirmar que la

---

p. 35. En efecto, se trata de un delito que combina la técnica del tipo del § 263 a del *StGB* ("Computerbetrug"), con la que se la del tipo de administración desleal del § 266 del mismo Código. Véase, a modo de ejemplo: Tröndle, Herbert - Fischer, Thomas, *Strafgesetzbuch und Nebengesetze* (53ª edición, München, Beck, 2006), pp. 1717 ss. y 1779 ss. Si en la actualidad se contara con un precepto de estas características no habría dificultades en importar al funcionario de una institución de previsión, encargado de un sistema informático de pagos, o bien, al empleado del departamento de remuneraciones de una empresa que efectúa manipulaciones al sistema de pago ordenando la emisión de cheques a terceros produciendo perjuicio al patrimonio de la entidad. En la actualidad, tales conductas no pueden calificarse de apropiación indebida, encuentran dificultes de encuadre en los delitos informáticos, menos podrían constituir estafa y similares cuestionamientos a los indicados se extienden para su calificación a título de hurto. Así, por ejemplo, la Sentencia de la Corte de Apelaciones de Santiago, 31 de mayo 2010, rol Nº 501-2010.

[73] Velasco Núñez, *Estafa informática*, cit. (n. 14), pp. 25 ss.

[74] Véase el Decreto con fuerza de ley Nº 3, de 20 de junio 2006, del Ministerio de Economía que fija el texto refundido y sistematizado de la Ley Nº 19.036 sobre propiedad industrial.

respuesta que ofrece nuestro *Código Penal* es deficiente y requiere *de lege ferenda* una reforma urgente para dar respuesta a estas nuevas formas de ataques contra el patrimonio que tienen lugar a través de la utilización ilícita de claves de acceso a banca *online,* que afectan la confianza y seguridad del mercado en las transacciones patrimoniales. Según se ha expuesto tal comportamiento constituye la esencia tanto del "phishing" como del "pharming" y, al mismo tiempo, es el sustrato fáctico sobre el cual desarrollaremos los problemas de imputación a título de estafa. Empero, los cuestionamientos son múltiples y no se agotan en este punto, porque hay otros asuntos relativos a la calificación jurídico-penal que merecen las etapas previas y posteriores al momento en que se produce el perjuicio patrimonial para el cuentacorrentista.

En efecto, según se ha expuesto y se deduce de los casos reseñados, la obtención ilícita de datos confidenciales asociados a cuentas bancarias, ya sea a través del envío masivo de correos electrónicos a los usuarios de Internet solicitando las claves y números secretos de cuentas corrientes, aparentando proceder del banco ("phishing"), o bien, mediante el acceso al sistema informático personal del usuario para desviar y cambiar la direcciones electrónicas contenidas en el servidor DNS para redirigir al usuario a una página falsa que simula ser la del banco ("pharming"), requiere de la existencia de una organización criminal más o menos compleja, generalmente, de carácter transnacional, cuya existencia frente a la ausencia de tipificación expresa de estas conductas, como también, a la falta de acuerdos de cooperación internacional en estas materias, hacen difícil su persecución. Además, de lo relativo a las conductas que constituyen una afectación clara de la intimidad de las personas en relación con los datos contenidos en sistemas informáticos y la existencia de intereses de naturaleza comercial que se ven comprometidos por la clara utilización maliciosa de la imagen de las entidades bancarias, hay otros hechos que tienen lugar con posterioridad que requieren también de una respuesta expresa, como la conducta del mulero contactado por la organización para transferir a cuentas de terceros en el extranjero los dineros que han sido obtenidos en actividades de apoderamiento patrimonial ilícito, cuya imputación penal según lo visto resulta altamente dudosa en Chile.

Realizadas estas precisiones la duda se concentra aquí, finalmente, en si es factible imputar estafa a quienes realizan las conductas de "phishing" y el "pharming". A ello se dedican los epígrafes que siguen.

1. *El punto de partida: el engaño en el modelo de estafa del "Código Penal".*

De los sistemas legislativos que podrían haberse tenido como referencia para la configuración de la estafa, en especial, la normativa del *Código Penal* español de 1822, o bien, la fuente más próxima aquí de éste que fue el *Code*

Pénal francés de 1810, nuestro Derecho se acogió al sistema casuístico del *Código Penal* español de 1848-1850, copiándolo casi literalmente[75].

Para nosotros vale algo más que la calificación de "notable retroceso" que en su oportunidad realizara Antón Oneca[76] en cuanto indicó que el *Código Penal* español de 1848-1850 implicaba una vuelta a la antigua legislación española, en especial, porque nosotros pasamos sin hacer mucho caso de las referencias comparativas que aparecían extractadas en los comentarios de Pacheco[77] que fue el texto al que Comisión Redactora echó mano para la elaboración de nuestro *Código Penal*[78]. Y, más que un retroceso resulta desconcertante que estas normas se mantengan todavía vigentes sin alteraciones de fondo, no sólo por su notable ambigüedad, falta de conceptualización, sino que, también, entre otras cosas por la ausencia de criterios claros de distinción entre la figura penal del artículo 468 y la del artículo 473[79]. Es que más allá de los argumentos que a favor o en contra y que por vía interpretativa puedan darse para calificar uno u otro de tipo penal como "el verdaderamente subsidiario" o "residual" en aras de salvar en algo la coherencia técnica, nos parece que el sistema no sólo no otorga seguridad jurídica, sino que su principal virtud original, esto es, los mentados "ejemplos" son hoy su principal defecto por cuanto se han vuelto anacrónicos e inservibles como métodos limitativos de las acciones que adquieren relevancia jurídica por la vía de la paráfrasis cualitativa de sus propios preceptos.

Así las cosas, frente a la ausencia de una respuesta penal expresa para los fraudes informáticos de apoderamiento patrimonial que permita abarcar los problemas a los que aquí nos enfrentamos, debemos necesariamente

---

[75] Schlack Muñoz, Andrés, *El concepto de patrimonio y su contenido en el delito de estafa*, en *Revista Chilena de Derecho*, 35 (2008) 2, p. 261; Fernández, *Engaño*, cit. (n. 45), p. 182; Hernández, Héctor, *Aproximación a la problemática de la estafa*, en AA.VV. *Problemas actuales de Derecho penal* (Temuco, Universidad Católica de Temuco, 2003), pp. 151-152; Garrido Montt, *Derecho penal*, cit. (n. 22), pp. 325-326.

[76] Lo que venía motivado en la idea de que se alteró el concepto general de estafa de inspiración francesa, no sólo porque no se ubicó al principio de la serie, sino también, porque se desnaturalizó su contenido, que hacía referencia clara al engaño y al error, integrándose por otras disposiciones la expresa mención a que el autor consiga una disposición patrimonial con ello. Además, asumía una exagerada casuística, mecanizando la penalidad en función de la cuantía de la defraudación; sobre todo lo cual, véase: Oneca, Antón, voz "Estafa", en Mascareñas, Carlos (director), *Nueva Enciclopedia Jurídica* (Barcelona, Francisco Seix, 1958), IX, p. 60.

[77] Pacheco, Joaquín Francisco, *El Código Penal, concordado y comentado* (6ª edición, Madrid, Imprenta y Fundición de Manuel Tello, 1888), III, pp. 345 ss.

[78] Véase: Rivacoba y Rivacoba, Manuel, *Evolución histórica del Derecho penal chileno* (Valparaíso, Edeval, 1991), p. 49.

[79] Sobre esto véase más arriba la nota 45.

recurrir al concepto general de estafa para así, desde ese lugar, establecer la eventualidad de la inclusión de estos hechos en el *Código Penal*.

Al respecto, anticipamos que no se comparte aquí la opinión de un sector de la doctrina que estima que el tipo penal del artículo 473 CPen. es suficiente para abarcar los casos de estafa informática que se regulan en el Derecho comparado, porque a nuestro juicio nos parece una tesis un tanto apresurada, en especial, porque los autores que a favor de ella se han pronunciado la sostienen de un modo muy general, sin someter a un juicio exhaustivo de valoración jurídico-racional la virtualidad de tales opiniones, en especial, frente a los múltiples casos de manipulación de datos contenidos en sistemas informáticos que se presentan en la cotidianeidad y que repercuten en perjuicios patrimoniales[80]. En efecto, una argumentación en sentido fuerte exige hacerse cargo aquí de estas cuestiones prácticas desde la dogmática misma de la estafa, sometiendo a su consideración exhaustiva la concurrencia o exclusión de sus elementos conceptuales.

Desde la aportación que en este ámbito efectuó Antón Oneca al definir la estafa como "la conducta engañosa, con ánimo de lucro injusto, propio o ajeno, que, determinando un error en una o varias personas, les induce a realizar un acto de disposición, consecuencia del cual es un perjuicio en su patrimonio o en el de un tercero"[81], hay un relativo consenso doctrinal y jurisprudencial sobre este punto[82]. No es el momento para intentar otra definición ni una reconstrucción del contenido conceptual, pero sí reclamar para que *de lege ferenda* ambas cuestiones tengan lugar, por la incapacidad que tiene esta aproximación para hacer ser frente a los cambios originados en las manifestaciones que adopta el engaño con motivo de las nuevas formas de interacción y comunicación que en la actualidad no necesariamente se

---

[80] La aportación de Balmaceda parece fundamental en este punto, pero con el respeto que merece su obra, se trata de una tesis doctoral dedicada al Derecho español con notas marginales de Derecho chileno. En cuanto a las observaciones que realizan Politoff, Matus y Ramírez relativas a la similitud de nuestro ordenamiento con la indeterminación de las formas de engaño que se contienen en el concepto general de estafa del Código Penal alemán, habría que objetar que ello no tiene en cuenta la dogmática desarrollada en dicho país en torno al concepto de fraude computacional contenido, a reglón seguido, en el §263a del Código Penal alemán. Véase, Balmaceda, *El delito*, cit. (n. 24), p. 121. Politoff - Matus - Ramírez, *Lecciones*, cit. (n. 24), p. 417. Cfr. Tröndle - Fischer, *Strafgesetzbuch*, cit. (n. 72), pp. 1717 ss.

[81] Oneca, *Estafa*, cit. (n. 76), p. 57.

[82] Es un consenso que podríamos calificar como relativo en cuanto a sus elementos, sin perjuicio, del contenido conceptual diferenciado de cada uno de ellos. Véase, por todos, la completa obra de Balmaceda, *El delito*, cit. (n. 45), pp. 21, 39, 43 y 62 ss. También es esencial Balmaceda Hoyos, Gustavo, *El delito de estafa en la jurisprudencia chilena*, en *Revista de Derecho*, 24 (Valdivia, 2011) 1, pp. 63 ss.

dan siempre entre personas de un modo directo o triangular, en especial, por el surgimiento de la obligación de cumplimiento de determinados deberes especiales, como también, de nuevos peligros en el marco de las complejas tecnologías, lo que demanda un concepto más sintético y diferenciado por ámbitos o formas específicas en que pueden tener lugar las múltiples manifestaciones de fraudes[83].

En este orden de apreciaciones, el relativo consenso doctrinal de mínimos consistiría aquí en que, por un lado, el engaño es el elemento caracterizador y diferenciador de la estafa respecto de otras figuras de enriquecimiento ilícito patrimonial, porque en este delito el sujeto activo no tiene otro compromiso con la acción que el de lograr que el tenedor o poseedor de la cosa se la entregue a consecuencia del engaño para así hacerla suya y, por el otro, que el engaño constituye el "primer elemento" en la serie de actos que desencadenan la relevancia penal de todas las modalidades de estafa del *Código Penal*, ya sean calificadas, básicas o residuales. Ahora bien, nos interesa destacar aquí que el engaño es lógicamente más evidente en los supuestos en que se realizan hechos o actos de materialización explicita, en cuanto no dicen relación con la realidad y, por ello, se les da el nombre de semánticos porque exigen una puesta en escena; por el contrario, no es tan evidente en los denominados engaños pragmáticos donde de lo que se trata es de interpretar relaciones de naturaleza contractual en las que no se expresa nada falso, sino que se oculta el propósito inicialmente exigible de comportarse de acuerdo con la calidad de contratante y, al no decir nada, se termina defraudando. De este modo, la diferencia entre el incumplimiento civil y la estafa quedaría fijada por la

---

[83] La idea cada vez más creciente de la existencia de deberes especiales era ajena a los modelos de estafa del siglo XIX. En efecto, estos se basaban en la existencia de relaciones de comunicación directa entre seres humanos, ya sean bilaterales o trilaterales. En la medida en que se avanzó a la sociedad postindustrial el tipo penal clásico de estafa se mostró insuficiente, por ejemplo, para dar respuesta a problemas como la declaración falsa de patrimonio para constituir una sociedad, las afirmaciones falsas que se hacen con fines publicitarios, el abuso por parte de los consumidores en la confianza depositada en el crédito y, también, en la existencia de "engaños" que tienen lugar por la manipulación de datos que inducen a "error" a un sistema de tratamiento de datos. Todas estas nuevas formas de estafa se estatuyen en la actualidad en Alemania como delitos de infracción de deberes especiales y bajo la forma de delitos de peligro abstracto. Lógicamente, que ello sea así conforme a la interpretación actual del § 263 *StGB* no quiere decir que lo sea también para el modelo del *Código Penal* chileno, ni siquiera *de lege data*. Véase: Tiedemann, Klaus, *Manual de Derecho penal económico. Parte general y especial* (Valencia, Tirant lo Blanch, 2010), pp. 209-210. Esta idea repercute por ejemplo en el contenido conceptual del perjuicio como elemento de la estafa. Véase al respecto: Balmaceda Hoyos, Gustavo - Ferdinand Peller, Michael, *Análisis dogmático del concepto de "perjuicio" en el delito de estafa*, en *Revista de Estudios de la Justicia*, 7 (2006), pp. 193 ss.

acreditación del incumplimiento *ab initio* de celebrar un contrato faltando al deber de decir verdad porque desde un principio no existió el propósito de cumplir con las obligaciones contractuales que se derivarían del mismo, logrando de este modo disposiciones patrimoniales; *a contrario sensu*, si la defraudación a través del incumplimiento de las obligaciones surge durante la ejecución del contrato civil o comercial, entonces, no hay estafa, sino sólo responsabilidad contractual[84].

El problema consiste en determinar cuándo podemos decir que estamos en presencia de un engaño que pueda interpretarse inequívocamente como un hecho o acto falso y sobre la base de qué parámetros sería factible sostener que una afirmación mendaz expresada al inicio de una relación contractual de orden civil o comercial, puede significar una estafa. Ello precisa pronunciarse sobre si la afirmación mendaz o la mera mentira, puede o no ser constitutiva de engaño y, al mismo tiempo, esbozar nuestra posición sobre la cuestión de la relevancia y la posición de la víctima, como también, sobre el problema de la categorización del error como elemento autónomo.

Las aproximaciones a estas cuestiones en nuestra doctrina distan mucho de ser calificadas como un paraje donde sea posible hallar un relativo consenso. En efecto, se dice, por un lado, que el derecho no puede hacerse cargo de proteger a los crédulos o débiles de espíritu (toda persona racional y prudente colocada en la situación de la víctima sabe o debería saber, en determinados contextos sociales, que las zarigüeyas se hacen las muertas)[85], por lo que la mera mentira no puede constituir una estafa ni aún a título de tentativa y, por el otro, que el engaño debe ser –siguiendo a la doctrina española– un engaño relevante con un contenido normativizado, a lo que se responde que en realidad es el error el que debe ser relevante y que no es necesario aquí recurrir a exigencias calificadas de "orientaciones políticas" sobre el contenido del engaño, lo que se cierra con la idea de que el error no es en realidad un elemento de la estafa, como tampoco lo serían el ánimo de lucro ni el perjuicio en la medida en que la ley no los exige[86]. Así, puede

---

[84] Escéptico sobre esta necesidad de delimitación, por ejemplo: Hernández, *Aproximación*, cit. (n. 75), p. 158.

[85] Para una descripción del contenido del engaño en el Derecho alemán y español, además, de la denominada normativización del mismo, véase: Pastor Muñoz, Nuria, *La determinación del engaño típico en el delito de estafa* (Madrid, Marcial Pons, 2004), pp. 27 ss.; Mayer Lux, Laura, *El actuar de la víctima en el delito de estafa. En especial sobre el principio de autoprotección y los deberes de veracidad*, en *Delito, pena y proceso. Libro Homenaje a la memoria del profesor Tito Solari Peralta* (Santiago, Editorial Jurídica de Chile, 2008), pp. 384 ss.: "La idea que subyace tras este planteamiento es la de exigir a toda persona un mínimo de nivel de diligencia en la custodia de sus propios bienes frente a posibles daños".

[86] Así, Hernández, Héctor, *Normativización del engaño y nivel de protección de la*

verse como en este delito no cobran mucho valor las afirmaciones prejuiciadas tan comunes sobre que aquí está todo dicho y que no hay nada que aportar, porque como puede advertirse queda bastante por avanzar en la línea de ayudar a la solución de los casos prácticos, en especial, si parece no reconocerse que el engaño tiene múltiples posibilidades, más allá de las que el derecho expresamente pretende resolver o que se procure erradamente que está obligado a dar frente al llamado de la necesidad de imputar penalmente todos los tipos de fraude hasta el límite de tornar casi indiferenciable el delito civil del penal[87].

Lamentablemente, nosotros no nos sumamos desde una posición tradicional al debate, en la medida que entendemos que el concepto de engaño puede ser entendido desde la concepción significativa de la acción desarrollada por Vives Antón[88], en cuanto supera el entendimiento de los comportamientos humanos como movimientos humanos causales, o bien, como ejercicio de actividades finales (esto es, al margen de consideraciones de orden ontológico o naturalístico), para pasar a interpretar los hechos o actos humanos a partir del sentido que se les atribuye conforme a procesos de comunicación intersubjetiva, donde cobran una especial relevancia los significados objetivos que se le confieren a los comportamientos en los contextos sociales en que tienen lugar, en la medida en que sólo pueden ser interpretados y comprendidos conforme a ellos. Así, de acuerdo a esta concepción la atribución de la acción de engaño en el delito de estafa y, al mismo tiempo, su relevancia jurídica para el Derecho penal viene dada por el significado que se le otorgue a la acción realizada en un determinado contexto social, es decir, que para afirmar que existe un engaño que cumple con la pretensión de relevancia penal, lo primero es poder afirmar que ese determinado hecho o acto es susceptible de ser conceptualizado inequívocamente como tal en el contexto de comunicación que ha tenido lugar[89].

En consecuencia, aquí de lo que se trata es de lograr en el engañado la

---

víctima en la estafa: *lo que dice y no dice la dogmática*, en *Revista Chilena de Derecho*, 37 (2010) 1, pp. 12 ss.

[87] Sobre esta cuestión de los prejuicios y de las exigencias a las que se enfrentan los "consensos" de la estafa, son esclarecedoras las palabras del prólogo de Quintero Olivares, Gonzalo a Valle Muñiz, José Manuel, *El delito de estafa*: *delimitación jurídico-penal con el fraude civil* (Barcelona, Bosch, 1987), pp. 11-14.

[88] Vives Antón, Tomás Salvador, *Fundamentos del sistema penal*. *Acción significativa y derechos constitucionales* (2ª edición, Valencia, Tirant lo Blanch, 2011), pp. 219 ss.

[89] Sobre esta concepción, además, pueden verse: Martínez-Buján Pérez, Carlos, *Derecho penal económico y de la empresa*. *Parte general* (2ª edición, Valencia, Tirant lo Blanch, 2011), p. 33 ss.; González Cussac, José Luis - Orts Berenguer, Enrique, *Compendio de Derecho penal*. *Parte general* (3ª edición, Valencia, Tirant lo Blanch, 2011), pp. 210 ss.; Martínez-Buján Pérez, Carlos, *El contenido de la anti-*

falsa representación de un hecho o de un acto, ya sea a través de la mentira o de cualquier otro medio que en la situación concreta pueda resultar eficaz para lograr una disposición patrimonial[90]. En este orden de consideraciones, ha de indicarse que el engaño no puede ser comprendido sin la referencia al error, porque ambos expresan o son parte de un único y complejo proceso de comunicación interpersonal donde las relaciones originadas y derivadas en el lenguaje –en la comprensión del sentido de acciones intersubjetivas–, cobran relevancia penal en la medida en que un sujeto decide utilizar ese enunciado con conocimiento de que ello tiene en un contexto sociocultural determinado la idoneidad suficiente para desinformar a otro o hacerle creer algo que no es verdad determinándole a realizar por sí o por intermedio de otro un acto que implica una disminución patrimonial.

De este modo, no resultan ser típicamente relevantes los engaños que no son capaces de producir un error, porque faltaría una parte del proceso de interacción y comunicación, en consecuencia, no pueden ser constitutivas de estafa aquellas manifestaciones del lenguaje que refuerzan en otro el error en el que se encuentra, porque no se da el proceso de inducción a la atribución de un sentido diverso del que realmente tiene un hecho o acto determinado, es decir, falta el necesario contraste entre la información previa y la contextual. De ahí que para determinar si la mentira es constitutiva de engaño más que recurrir a contextos normativos extrapenales, en especial, de orden civil para establecer algún criterio que permita decidir si la declaración mendaz contenida en un documento, acto o hecho merezca la calificación de antijurídica *per se* conforme a cualquiera otra rama del ordenamiento jurídico, de lo que se trata aquí es de introducir un criterio de valoración-adecuación que, independiente de todas esas cuestiones, permita afirmar de un modo inequívoco, sobre la base de criterios derivados de significados en contextos socioculturales específicos, que la información que recibió un sujeto objetivamente merece la calificación de suficiente para que cualquier persona en su situación le imputara un contenido de verdad o certeza sin serlo. Ello, requiere de un análisis del mensaje que ha de ser contrastado con la información previa que disponía el sujeto, además, de su información contextual relativa al caso concreto y el comportamiento del emisor y del receptor del mensaje; en consecuencia, engaño-error constituyen un único proceso de comunicación que se funden en la acción significativa constitutiva de estafa[91].

---

juridicidad. Un estudio a partir de la concepción significativa del delito (Valencia, Tirant lo Blanch, 2013), pp. 15 ss.

[90] Vives Antón, Tomás Salvador González Cussac, José Luis, *De las defraudaciones*, en AA.VV., *Comentarios al Código Penal de 1995* (Valencia, Tirant lo Blanch, 1996), II, p. 1215 ss.

[91] Se trata de una aproximación desde la filosofía del lenguaje, la pragmática y, en

En este entendimiento de las relaciones de imputación que en el fondo consiste en la introducción de un criterio de adecuación para determinar en qué momento es posible afirmar que estamos en presencia de al menos una tentativa de estafa, puede presentarse como una alternativa, con alguna lógica profundización posterior, frente a los tradicionales criterios que buscan responder al problema de la adecuación desde la óptica de los deberes de autoprotección de la víctima, que Hernández critica por el excesivo subjetivismo[92]. En efecto, una de las principales virtudes de la concepción significativa del delito, es el superar el extremo subjetivismo del finalismo y también su capacidad para apartarse del criterio cronológico causalista, lo que aquí se traduce en la exclusión de la concepción que como antecedente y consecuente tienen el engaño y el error en la aproximación tradicional de la estafa, para pasar a ser un todo único de relación de comunicación donde la relevancia y la atribución de sentido depende del contexto completo en que se desarrolla el lenguaje.

Ahora, no sólo es posible desde la concepción de Vives Antón superar la cuestión del clásico argumento del "óbice cronológico" y facilitar de este modo la eventualidad de la comisión por omisión, en los contextos en que existe un deber de sacar a la víctima del error en que se encuentra, sino que, al mismo tiempo, excluye el ánimo de lucro como elemento subjetivo del tipo de estafa y lo traslada a la valoración de la acción misma. En efecto, el dolo es en la concepción significativa de la teoría del delito es un compromiso con la acción[93], con independencia de ese "algo" que está detrás –lo interno o psicológico cuestión que no vemos ni interesa al derecho porque no se puede probar–, el dolo no está fuera de la acción porque pertenece a

---

especial, aquí desde la teoría de la relevancia. Véase: Wilson, Deidre - Sperber, Dan, *La teoría de la relevancia*, en *Revista de Investigación Lingüística*, 7 (2004), pp. 233-282. También: Camacho, Victoria, *Mentiras*, *relevancia y teoría de la mente*, en *Pragmalingüística*, 13 (2005), pp. 51-64. También, desde la teoría del lenguaje y la pragmática, pero desde una óptica dogmática diferente puede verse el capítulo 1.2. titulado "Begründung des Ausgangspunkts: Betrug und Sprechakttheorie," del libro de Mayer Lux, Laura, *Die konkludente Täuschung beim Betrug* (Göttingen, Bonn University Press, 2013), pp. 16 ss.

[92] Hernández, *Normativización*, cit. (n. 86), pp. 17 ss.

[93] González Cussac, José Luis, "*Dolus in re ipsa*", en Carbonell Mateu, Juan Carlos - González Cussac, José Luis y otros (directores) y Cuerda Arnau, María Luisacoordinadora), *Constitución*, *derechos fundamentales y sistema pena*. *Semblanzas y estudios con motivo del setenta aniversario del profesor Tomás Salvador Vives Antón* (Valencia, Tirant lo Blanch, 2009), pp. 818 ss.; Martínez-Buján, Carlos, *El concepto "significativo" de dolo*: *un concepto volitivo normativo*, en *Problemas actuales del Derecho Penal y de la Criminología*. *Estudios penales en memoria de la profesora María del Mar Díaz Pita* (Valencia, Tirant lo Blanch, 2008), pp. 324 ss.

la interpretación del sentido de la misma, conforme al contexto de comunicación en que ha tenido lugar, por ende, los ánimos no tienen importancia porque no se pueden acreditar en el proceso penal, no es posible "saber" o "conocer" por inferencia lo que pensaba el sujeto, ni mucho menos cuales son o eran sus intenciones.

Así las cosas, al pasar a formar parte de la acción misma esos elementos subjetivos tienden a objetivarse, porque lo importante deja de ser si el sujeto obró con un determinado ánimo que complementa o integra el elemento subjetivo del injusto (como ocurre en la estafa con el citado ánimo de lucro), sino que se convierten en la atribución de sentido que pueda dársele en el contexto comunicativo a la acción misma, es decir, ese "ánimo" tal como las palabras tiene un significado objetivo y no depende de la intención con que se pronunciaron[94]. Con ello, el denominado elemento "ánimo de lucro" no es tampoco distinto del engaño y, por ende, pertenece a ese complejo proceso de comunicación donde tampoco el error puede entenderse como un elemento diferenciado del significado de la acción. En consecuencia, a ese proceso de relación/interrelación que es el engaño y el error debe ser posible atribuirle *ex ante* socialmente un significado inequívoco de utilidad o beneficio, directo o indirecto, incluso aunque careciera finalmente *ex post* de valor económico, a título de perjuicio.

Entendemos que, al menos por el momento, para que sea posible afirmar la presencia de una estafa en el modelo del *Código Penal*, debe estar siempre presente una relación entre personas, porque sólo 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. Si en alguna parte de ese proceso interfiere la manipulación de un sistema de tratamiento de datos, o bien, es un programa computacional el que logra disposiciones patrimoniales por parte de personas, entonces, no hay engaño ni error en el sentido expuesto, no hay ni siquiera ese "cualquier otro engaño semejante" (artículo 468), ni ese "usando de cualquier engaño" (artículo 473) a los que alude el *Código Penal* en la regulación actual de la estafa.

Así, mientras no exista una regulación expresa de la estafa informática comprensiva de los fraudes antes descritos, con la suficiente flexibilidad para hacerse cargo de otros que puedan tener eventualmente lugar a través de la utilización indebida de las plataformas de banca "online" para apoderamientos de dineros en cuentas corrientes, todas las cuestiones expresadas son atípicas en el modelo de la estafa común del *Código Penal*[95].

---

[94] González Cussac - Orts Berenguer, *Compendio*, cit. (n. 89), p. 240.

[95] Así, por una regulación expres:a Mera Figueroa, *Delitos*, cit. (n. 24), p. 54.

2. *Punibilidad del "phishing": los problemas del engaño, el error y la disposición patrimonial.*

Las formas de engaño a que alude el *Código Penal* precisan como un requisito *sine qua non* la existencia de una interrelación caracterizada por la interpretación del sentido de determinadas acciones, cuestión que si bien es un proceso que puede eventualmente ser averiguado conforme a un baremo objetivo *ex ante* o no, lo cierto es que siempre precisa de una interlocución entre sujetos, por un lado, quien engaña al crear situaciones fingidas o realizar maniobras fraudulentas, atribuir cualidades falsas, utilizar nombres supuestos, simular, deformar u ocultar hechos ciertos, etc., y, por la otra, un engañado que le atribuye a ello un significado diverso del que en un contexto normal de comunicación le hubiere asignado.

Esta tesis permite excluir la posibilidad de imputación penal de la estafa informática en sentido tradicional o estricto, esto es, la que tiene lugar a través del engaño a máquinas o sistemas de tratamiento automatizados de información. En efecto, conforme a lo expuesto en la concepción significativa de la acción el engaño a que alude nuestro *Código Penal* ha de producir un error en un sujeto con capacidad de atribuirle sentido a las acciones que ocurren en contextos de comunicación interpersonal; en consecuencia, una máquina o un sistema informático no puede ser "otro", porque sólo puede serlo una persona[96].

Ahora bien, a diferencia de la estafa informática clásica en el "phishing" aparece un grado mínimo de interacción y comunicación entre personas, desde el momento en que aquí las claves son facilitadas por una persona a consecuencia de un proceso de comunicación puesto en marcha por otra, caracterizado por la representación de imágenes o mensajes vía correo electrónico solicitando datos. Sin embargo, ello no tiene lugar en todos los casos, porque es un hecho que una de las variantes de este tipo de fraude consiste en introducirse en el computador personal de la víctima a través de una red de tratamiento común de información o valiéndose de Internet, con un virus que registra todas las pulsaciones que se hacen en el teclado, las que memoriza en un fichero y remite como registro de secuencias al sujeto que introdujo estos "malware" llamados "keyloggers" quien, posteriormente, las decodifica buscando datos que den cuenta de tecleos de acceso a banca electrónica con la consecuente sustracción de las claves personales[97]. En este último caso, claramente no hay interacción ni comunicación personal y, por ende, no hay ni la más elemental forma de engaño de la estafa.

---

[96] Gutiérrez Francés, *Fraude*, cit. (n. 71), pp. 36 ss.; Mata y Martín, *Estafa*, cit. (n. 12), p. 41.

[97] Gallego Soler, *Arts. 234*, cit. (n. 37), p. 554.

Ahora bien, en la modalidad más común de "phishing" (en la que se solicitan claves por correo), ese mínimo de comunicación exigible para afirmar la relevancia típica podría estar presente, en la medida en que dependiendo de la idoneidad y características del contenido sea posible sostener que hay un mensaje inequívocamente mendaz y un receptor del mismo que lo ha decodificado de un modo erróneo. Sin embargo, lo que aquí sucede es, por una parte, que la persona que sufre el error no es quien realiza el acto de disposición patrimonial como se exige en el modelo tradicional de estafa del *Código Penal*, sino que ésta solamente entrega la clave de acceso al sistema de tratamiento de datos, siendo el propio sujeto activo quien una vez al interior de la plataforma bancaria realiza el acto de disposición patrimonial. Por otra parte, incluso la diferencia con la estafa informática clásica resulta evidente porque en este caso el acto de disposición no lo realiza un sistema informático o la máquina a consecuencia de las manipulaciones directas por parte del sujeto activo.

Sin perjuicio, de que se ha argumentado que no obsta a la apreciación de estafa la circunstancia que la disposición patrimonial sea ejecutada por un sujeto diferente del que es directamente inducido a un error, el asunto aquí es que el engaño no se produce sobre una cosa susceptible de valoración económica, sino que sobre la clave de acceso al sistema informático. En efecto, el "engañado" lo que entrega es la clave y no el dinero que se encuentra depositado en la cuenta. Sin perjuicio de lo indicado anteriormente, en relación con la atipicidad de la suplantación de identidad informática, en este caso lo que tiene lugar a través de la entrega de la clave secreta, en cuanto posibilita el acceso a la banca *online*, es el apoderamiento de un mecanismo que, según ha observado nuestra Superintendencia de Bancos e Instituciones Financieras[98], es equivalente a la firma electrónica reconocida en las letras f) y g) del artículo 2 de la Ley Nº 19.799, de 12 de abril de 2002, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma[99].

En tal entendido, la firma electrónica incorporada a un documento, título o valor produce los mismos efectos que el acto celebrado en papel (por ejemplo, el librar un cheque), por ello, la clave en sí misma otorga a su titular el poder de realizar transferencias electrónicas que de otra forma debería realizar materialmente a través de la firma, elemento esencial para

---

[98] Budenevich Le-Fort, Carlos, *Invitación a la Comisión de Economía, Fomento y Desarrollo de la Cámara de Diputados. Operación del sistema "Pinpass" en tarjetas de crédito. Presentación del Superintendente de Bancos e Instituciones Financieras* (Valparaíso, 8 de junio 2010) [visible en Internet: http://goo.gl/5Vwkp].

[99] El artículo 2 de la Ley Nº 19.799 dispone que: "*para los efectos de esta ley se entenderá por: f) firma electrónica: cualquier sonido, símbolo o proceso electrónico, que permite al receptor de un documento electrónico identificar al menos formalmente a su autor*".

la validez de las operaciones con títulos de crédito o valores. Sin embargo, sólo equivale a la firma y no al título mismo y, por ende, la clave en sí misma considerada carece de valor patrimonial, en cuanto en sí misma considerada no tiene incorporada derechos de tal naturaleza.

De esta forma, siguiendo la doctrina de Vives Antón y González Cussac del grado de incorporación del derecho al título[100] que la contiene, hay que concluir que en este caso el apoderamiento de la clave bancaria válida, que posibilita el acceso a un sistema de transferencia patrimonial de activos y que permite la subscripción de un documento equivale a una firma electrónica y, en concreto, otorga acceso a librar un título que puede ser equivalente a la disposición patrimonial de todos los activos que se encuentran en la cuenta corriente. Sin embargo, la sola tenencia de la clave no implica la disponibilidad inmediata de los dineros en depósito, cuestión que sí tiene lugar cuando se completa la transferencia de activos a la cuenta de un tercero, momento en que el autor realiza un acto que comercialmente equivale a librar un documento de pago.

Así las cosas, al menos en lo que se refiere al "phishing" no sería posible siguiendo este criterio establecer la posibilidad de imputación a título de estafa tradicional. Según se ha dicho, por regla general, tiene lugar mediante el envío de correos electrónicos solicitando claves secretas bancarias a nombre de la entidad bancaria a la que pertenece el destinatario del mensaje, aduciendo motivos de seguridad, mejoras del servicio, mantenimiento, para una vez que se hagan constar defraudar a través de la realización de una transferencia a favor propio o de terceros. Pues bien, a los problemas relativos a la naturaleza de la clave en sí misma considerada, además, del hecho que no es quien sufre el error el que realiza el acto de disposición patrimonial, toda vez que el que lo efectúa es el mismo sujeto que ha inducido el "engaño", a través de una transferencia desde dentro de la misma plataforma informática, se le suma la cuestión de si hay un engaño típicamente relevante, en el envío masivo de correos, generalmente desde el extranjero, mal redactados y erróneamente traducidos, o bien, con remitentes desde dentro del país, pero con mensajes burdos, respecto de los cuales cualquier sujeto, en la mayoría de los casos, con una diligencia media se daría el tiempo de verificar. Aun aceptándose que la simple mentira en el caso concreto pueda dar lugar a un engaño, aquí faltarían el error y la disposición patrimonial[101].

Entendemos, desde la concepción que aquí se defiende que la mayoría de

---

[100] Vives Antón, Tomás Salvador - González Cussac, José Luis y otros, *Derecho penal. Parte especial* (3ª edición, Valencia, Tirant lo Blanch, 2010), p. 373; Azcona Albarrán, *Tarjetas*, cit. (n. 66), p. 101.

[101] En relación con la afirmación mendaz, ampliamente: Mera Figueroa, *Delitos*, cit. (n. 24), p. 69.

los casos de "phishing" no se incluyen en la categoría de engaños típicos, en la medida en que inequívocamente en nuestro contexto sociocultural puede afirmarse que eran susceptibles de ser evitados o prevenidos, siempre que sea posible afirmar *ex ante*, en el caso concreto y conforme a las circunstancias del hecho, que en la convivencia social ordinaria el común de los chilenos que tiene una cuenta corriente se representaría la duda sobre si pueden o no pedirle claves secretas por medio de correos electrónicos, en especial, cuando la prevención del fraude bancario en cuanto a educación del cuentacorrentista ha estado orientada en el último tiempo a informar sobre el hecho de que las entidades financieras no solicitan a sus clientes ningún tipo de claves de acceso a cuentas *online*. En consecuencia, tanto desde un punto de vista objetivo como en relación con los conocimientos personales exigibles al promedio de los eventuales afectados, teniendo en cuenta sus conocimientos personales, su experiencia y la totalidad de las circunstancias concretas que puedan rodear el hecho, entendemos que estamos en presencia de una conducta que al menos en la sociedad chilena no resulta ser un engaño en términos de comunicación significativamente relevante[102].

3. *El "pharming": un caso sin engaño ni error.*

Por último, esta conducta es un claro ejemplo de que la *praxis* ofrece supuestos que sin la más mínima simulación se logran revelaciones de claves de cuentas corrientes y, posteriormente, apoderamientos patrimoniales que tienen lugar a través de una manipulación desde dentro del sistema informático bancario, sin interacción comunicativa entre personas[103]. En el "pharming" derechamente lo que se realiza es una manipulación[104] sobre el sistema operativo informático tanto del titular de la clave bancaria, como también, de la plataforma de banca "online", en consecuencia, aquí no hay ni engaño ni error. En efecto, a través de esta técnica se altera un proceso electrónico en perjuicio del banco, faltando los elementos intelectuales propios

---

[102] Gallego Soler, José Ignacio, *Fundamento y límites de los deberes de autoprotección de la víctima en la estafa. Comentario a la STS 1217/2004, de 2 noviembre 2004*, en *Anuario de Derecho Penal y Ciencias Penales*, 58 (2005), pp. 541 ss.

[103] Tanto es así, que la jurisprudencia española ha incluido esta figura dentro de la expresión "otros artilugios semejantes", del artículo 248.2. Así, la Sentencia del Tribunal Supremo, 13 de junio 2007, Nº 533/07.

[104] Este término, si bien no se corresponde con el lenguaje técnico de la informática sí sirve para abarcar la mayoría de los supuestos en los cuales un sujeto "opera" un sistema de tratamiento de datos, consignado una transferencia no consentida de activos en perjuicio de otra persona. Sobre ello: Fernández Teruelo, Javier Gustavo, *Capítulo 31: estafas*, en Álvarez García, Francisco - González Cussac, José Luis (directores), *Comentarios a la Reforma Penal de 2010* (Valencia, Tirant lo Blanch, 2010), p. 280.

de la estafa tradicional, porque aquí lo que ocurre es que el usuario teclea en la barra de direcciones del navegador intentando ingresar a su banco, pero debido a que su computador ha sido infectado previamente con un virus, se redirige la navegación hacia una "web" falsa donde al intentar ingresar mediante la digitación de su clave de acceso está poniendo a disposición de los defraudadores sus datos bancarios, los que incluso pueden tener seguridad de que son ciertos, porque la página "web" falsa está programada para dar múltiples mensajes de error de acceso, lo que posibilita mediante la reiteración de la digitación una certeza e inmediatez en la obtención de todas las claves, incluyendo el "Pinpass". En efecto, a través de esta técnica, de modo paralelo se ingresa al sistema bancario realizando las transferencias de activos a cuentas que por regla general, según se ha apuntado, pertenecen a terceros (muleros)[105].

Puede verse como estas "maquinaciones" son verdaderos programas informáticos que tienen por objeto directo la obtención de claves, cuestión que en ningún caso puede considerarse un acto propio del delito de estafa, como tampoco, una manipulación de un sistema de tratamiento de datos, ya que se realiza con claves verdaderas[106].

Así las cosas, las posibilidades de una respuesta penal al "phishing" y "pharming" pasan por la incriminación de la creación de programas destinados a la comisión de delitos de estafa informática[107], asumiendo derechamente que acá hay que dar una especificidad a los medios de comisión en el entendido que aquí no sólo se relativiza la relación de alteridad propia de la estafa en sentido tradicional[108], desde que falta la existencia del trato físico real o visible entre el sujeto activo y la víctima y, también, reconociéndose la necesidad de dar una respuesta para los casos en los cuales falta tanto el

---

[105] Flores Prada, *Criminalidad*, cit. (n. 15), p. 211.

[106] Sobre estos problemas, Romeo Casabona, Carlos María - Sola Reche, Esteban - Sánchez Lázaro, Fernando y otros, *Informe sobre los nuevos instrumentos jurídicos en la lucha contra la delincuencia económica y tecnológica. Líneas de investigación y conclusiones*, en AA.VV., *Nuevos instrumentos jurídicos contra la delincuencia económica y tecnológica* (Granada, Comares, 2012), pp. 723-727.

[107] Esta es una de las novedades de la Ley Orgánica 5/2010, que introdujo en España la letra b) al citado artículo 248. 2 del *Código Penal* de 1995, que ha quedado del modo siguiente: "*También se consideraran reos de estafa*: a) *Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de un activo patrimonial en perjuicio de otro*. b) *Los que fabriquen, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este título*. c) *Los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero*".

[108] Así, Magliona - López, *Delincuencia*, cit. (n. 21), pp. 221 ss.

citado error como el engaño[109], puesto que lo que se altera, modifica o manipula indebidamente es un sistema informático para obtener beneficios de orden patrimonial[110].

V. Conclusiones

Después de haber transitado por las múltiples respuestas que ofrece nuestro Derecho para la sanción de las conductas que comentamos, las que en ningún caso se limitan a la mera discusión sobre la concurrencia de la estafa, estamos en condiciones de sostener que el estado actual de la legislación chilena en esta materia requiere de una adecuación necesaria y urgente que permita hacer frente a la necesidad de punición que reclaman los fraudes bancarios cometidos a través de la banca "online", en todas sus dimensiones.

Tal cuestión deviene de la imposibilidad de adecuación típica de los fraudes bancarios más comunes que se cometen en la actualidad, tanto en el modelo de estafa contenido en el *Código Penal*, como también, en las figuras penales especiales de la ley de delitos informáticos. Según hemos expuesto en detalle, actualmente en nuestro Derecho penal, el acceso ilegítimo a cuentas corrientes de terceros, a través de la plataforma de Internet de una entidad bancaria con la finalidad de transferir los dineros depositados o los créditos contenidos en ellas, resulta increíblemente para los tiempos que corren atípico, sin que sea posible recurrir a ninguna figura alternativa dentro de la legislación penal que permita hacer frente a las exigencias de protección de la seguridad en la transacciones comerciales y civiles que se realizan por Internet a través de instituciones bancarias.

Cualquier otra interpretación es, conforme a lo expuesto, una transgresión del principio de legalidad y una adecuación antojadiza de las normas penales existentes que, a falta de un precepto que específicamente dé una respuesta a estos problemas, produce sentencias contradictorias como las observadas que, sin duda, no ayudan a la necesaria seguridad jurídica que ha de existir en un Estado democrático de Derecho.

Bibliografía

AA.VV. *Problemas actuales de Derecho penal* (Temuco, Universidad Católica de Temuco, 2003).

---

[109] Gallego Soler, José Ignacio, *Arts. 234*, cit. (n. 37), pp. 550 y 552.

[110] Así, Romeo Casabona - Sola Reche - Sánchez Lázaro, *Informe*, cit. (n. 106), p. 729.

AA.VV., *Anteproyecto de Código Penal Chileno de 2005, elaborado por la Comisión Foro Penal*, en *Política Criminal*, 1 (2006).

Acum Maldonado, Carolina, *La responsabilidad civil de los prestadores de servicios en la sociedad de la información* en *Revista de Contratación Electrónica,* 115 (2011).

Argenti, Thais - Peleteiro, Almudena, *Luces y sombras de dos de los nuevos delitos introducidos con la reforma penal de 2010: el acoso laboral (mobbing) y el intrusismo informático*, en *Actualidad Jurídica*, 29 (2011).

Azcona Albarrán, Carlos, *Tarjetas de pago y Derecho penal. Un modelo interpretativo del artículo 248.2 c) del Código Penal* (Barcelona, Atelier, 2012).

Balmaceda Hoyos, Gustavo - Ferdinand Peller, Michael, *Análisis dogmático del concepto de "perjuicio" en el delito de estafa,* en *Revista de Estudios de la Justicia,* 7 (2006).

Balmaceda Hoyos, Gustavo, *El delito de estafa en la jurisprudencia chilena*, en *Revista de Derecho*, 24 (Valdivia, 2011) 1.

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

Balmaceda, Gustavo, *El delito de estafa: doctrina y jurisprudencia* (Santiago, Legal-Publishing, 2012).

Benítez Ortúzar, Ignacio, *Informática y delito. Aspectos penales relacionados con las nuevas tecnologías*, en Morillas Cueva, Lorenzo (directores), *Reforma del Código Penal. Respuestas para una sociedad del Siglo XXI* (Madrid, Dykinson, 2009).

Bolea Bardón, Carmen, *Arts. 197-216*, en Corcoy Bidasolo, Mirentxu - Mir Puig, Santiago, *Comentarios al Código Penal. Reforma LO 5/2010* (Valencia, Tirant lo Blanch, 2011).

Budenevich Le-Fort, Carlos, *Invitación a la Comisión de Economía, Fomento y Desarrollo de la Cámara de Diputados. Operación del sistema "Pinpass" en tarjetas de crédito. Presentación del Superintendente de Bancos e Instituciones Financieras* (Valparaíso, 8 de junio 2010) [visible en Internet: http://goo.gl/5Vwkp].

Bullemore, Vivian - Mackinnon, Jhon, *Curso de Derecho penal. Parte especial* (2ª edición, Santiago, LexisNexis, 2007), IV.

Cabrera Guirao, Jorge - Contreras Enos, Marcos, *El engaño típicamente relevante a título de estafa: modelos dogmáticos y análisis jurisprudencial* (Santiago, LegalPublishing, 2009).

Cajani, Francesco, *International* "phishing" *gangs and operation phish & chip*, en *Digital Evidence and Electronic Signature Law Review*, 6 (2009).

Camacho, Victoria, *Mentiras, relevancia y teoría de la mente*, en *Pragmalingüística,* 13 (2005).

Conte, Philippe, *Droit pénal spécial* (3ª edición, Paris, LexisNexis, 2007).

Escalona Vásquez, Eduardo, *El hacking no es (ni puede ser) delito*, en *Revista Chilena de Derecho Informático*, 4 (2004).

Etcheberry, Alfredo, *Derecho penal. Parte especial* (3ª edición, Santiago, 1998), III.

Etcheberry, Alfredo, *Derecho penal. Parte especial* (3ª edición, Santiago, Editorial Jurídica de Chile, 1998), IV.

Fernández Díaz, Álvaro, *Engaño y víctima en la estafa*, en *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, 26 (2005) I.

Fernández Teruelo, Javier Gustavo, *Capítulo 31: estafas*, en Álvarez García, Francisco - González Cussac, José Luis (directores), *Comentarios a la Reforma Penal de 2010* (Valencia, Tirant lo Blanch, 2010).

Fernández Teruelo, Javier, *Cibercrimen: los delitos cometidos a través de Internet* (Madrid, Constitutio Criminalis Carolina, 2007).

Flores Mendoza, Fátima, *Nuevas modalidades de fraude a la banca electrónica*, en *Nuevos instrumentos jurídicos contra la delincuencia económica y tecnológica* Granada, Comares, 2012).

Flores Prada, Ignacio, *Criminalidad informática. Aspectos sustantivos y procesales* (Valencia, Tirant lo Blanch, 2012).

Gallego Soler, José Ignacio, *Arts. 234-262*, en Corcoy Bidasolo, Mirentxu - Mir Puig, Santiago, *Comentarios al Código Penal. Reforma LO 5/2010* (Valencia, Tirant lo Blanch, 2011).

Gallego Soler, José Ignacio, *Fundamento y límites de los deberes de autoprotección de la víctima en la estafa. Comentario a la STS 1217/2004, de 2 noviembre 2004*, en *Anuario de Derecho Penal y Ciencias Penales*, 58 (2005).

Garrido Montt, Mario, *Derecho Penal. Parte especial* (4ª edición, Santiago, Editorial Jurídica de Chile, 2008), IV.

González Cussac, José Luis - Matallín Evangelio, Ángela y otros, *Esquemas de Derecho penal. Parte especial* (2ª edición, Valencia, Tirant lo Blanch, 2011).

González Cussac, José Luis - Orts Berenguer, Enrique, *Compendio de Derecho penal. Parte general* (3ª edición, Valencia, Tirant lo Blanch, 2011).

González Cussac, José Luis, "*Dolus in re ipsa*", en Carbonell Mateu, Juan Carlos - González Cussac, José Luis y otros (directores) y Cuerda Arnau, María Luisa (coordinadora), *Constitución, derechos fundamentales y sistema pena. Semblanzas y estudios con motivo del setenta aniversario del profesor Tomás Salvador Vives Antón* (Valencia, Tirant lo Blanch, 2009).

González Cussac, José Luis, *Tecnocrimen*, en González Cussac, José Luis - Cuerda Arnau, María Luisa (directores) y Fernández Hernández, Antonio (coordinador), *Nuevas amenazas a la seguridad nacional: terrorismo, criminalidad organizada y tecnologías de la información y la comunicación* (Valencia, Tirant lo Blanch, 2013).

Grisolía, Francisco, *La estafa procesal en el Derecho penal chileno*, en *Revista Chilena de Derecho,* 24 (1997) 3.

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

Hernández, Héctor, *La estafa triangular en el Derecho Penal chileno, en especial la estafa procesal,* en *Revista de Derecho*, 23 (Valdivia, 2010) 1.

Hernández, Héctor, *Normativización del engaño y nivel de protección de la víctima en la estafa: lo que dice y no dice la dogmática*, en *Revista Chilena de Derecho*, 37 (2010) 1.

Hernández, Héctor, *Perspectivas del Derecho Penal económico en Chile*, en *Persona y Sociedad*, 19 (2005) 1.

Hernández, Héctor, *Uso indebido de tarjetas falsificadas o sustraídas y de sus claves*, *Política Criminal*, 5 (2008).

Herzog, Félix, *Straftaten im Internet, Computerkriminalität und die Cybercrime Conventio*, en *Política Criminal*, 8 (2009) 4.

Huerta, Marcelo - Líbano, Claudio, *Delitos informáticos* (2ª edición, Santiago, Jurídica ConoSur, 1999).

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

Labatut, Gustavo - Zenteno, Julio, *Derecho penal. Parte especial* (7ª edición, Santiago, Editorial Jurídica de Chile, 2007), II.

Magliona Markovicth, Claudio - López Medel, Macarena, *Delincuencia y fraude informático. Derecho comparado y Ley Nº 19.223* (Santiago, Editorial Jurídica de Chile, 1999).

Martínez-Buján Pérez, Carlos, *Delitos relativos al secreto de empresa* (Valencia, Tirant lo Blanch, 2010).

Martínez-Buján Pérez, Carlos, *Derecho penal económico y de la empresa. Parte general* (2ª edición, Valencia, Tirant lo Blanch, 2011).

Martínez-Buján Pérez, Carlos, *El contenido de la antijuridicidad. Un estudio a partir de la concepción significativa del delito* (Valencia, Tirant lo Blanch, 2013).

Martínez-Buján, Carlos, *El concepto "significativo" de dolo: un concepto volitivo normativo*, en *Problemas actuales del Derecho Penal y de la Criminología. Estudios penales en memoria de la profesora María del Mar Díaz Pita* (Valencia, Tirant lo Blanch, 2008).

Mata y Martín, Ricardo, *Desarrollo tecnológico y legislación penal en defensa de los derecho de los creadores*, en *Nuevos instrumentos jurídicos contra la delincuencia económica y tecnológica* (Granada, Comares, 2012).

Mata y Martín, Ricardo, *Estafa convencional, estafa informática y robo en el ámbito de los medios electrónicos de pago. El uso fraudulento de tarjetas y otros instrumentos de pago* (Pamplona, Thomson Aranzadi, 2007).

Mayer Lux, Laura, *Die konkludente Täuschung beim Betrug* (Göttingen, Bonn University Press, 2013).

Mayer Lux, Laura, *El actuar de la víctima en el delito de estafa. En especial sobre el principio de autoprotección y los deberes de veracidad*, en *Delito, pena y proceso. Libro Homenaje a la memoria del profesor Tito Solari Peralta* (Santiago, Editorial Jurídica de Chile, 2008).

Mera Figueroa, Jorge, *Delitos contra la propiedad revisión crítica y propuestas de reforma*, en *Revista de Estudios de la Justicia*, 13 (2010).

Mera Figueroa, Jorge, *Fraude civil y penal. El delito de entrega fraudulenta* (Santiago, LexisNexis, 2001).

Miró Linares, Fernando, *Cibercrímenes económicos y patrimoniales*, en Ortiz Urbina, Iñigo (coordinador), *Memento práctico: Penal económico y de la empresa 2011-2012* (Madrid, Francis Lefebvre, 2011).

Monterde Ferrer, Francisco, *Especial consideración de los atentados medios informáticos contra la intimidad y la privacidad*, en *Delitos contra y a través de las nuevas tecnologías ¿Cómo reducir su impunidad? Cuadernos de Derecho Judicial,* 3 (2006).

Morales Prats, Fermín - Morón Lerma, Esther, *De los delitos relativos al mercado y a los consumidores*, en Quintero Olivares, Gonzalo (director) y Morales Prats, Fermín (coordinador), *Comentarios al Código Penal español* (6ª edición, Pamplona, Aranzadi, 2011), II.

Morales Prats, Fermín, *Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio*, en Quintero Olivares, Gonzalo (director) - Morales Prats, Fermín (coordinador), *Comentarios al Código Penal español* (6ª edición, Pamplona, Aranzadi, 2011), I.

Morón Lerma, Esther, *Internet y Derecho penal: "hacking" y otras conductas ilícitas en la red* (Pamplona, Aranzadi, 1999).

Muñoz Conde, Francisco, *Derecho penal. Parte especial* (18ª edición, Valencia, Tirant lo Blanch, 2010).

Oneca, Antón, voz "Estafa", en Mascareñas, Carlos (director), *Nueva Enciclopedia Jurídica* (Barcelona, Francisco Seix, 1958), IX.

Orts Berenguer, *Delitos contra la libertad e indemnidad sexuales (II)*, en Vives Antón, Tomás Salvador, *Derecho penal. Parte especial* (3ª edición, Valencia, Tirant lo Blanch, 2010).

Pacheco, Joaquín Francisco, *El Código Penal, concordado y comentado* (6ª edición, Madrid, Imprenta y Fundición de Manuel Tello, 1888), III.

Pardo Albiach, Juan, *Ciberacoso: "cyberbullying", "grooming", redes sociales y otros peligros*, en González, Javier (coordinador), en *Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en Internet* (Valencia, Tirant lo Blanch, 2010).

Pastor Muñoz, Nuria, *La determinación del engaño típico en el delito de estafa* (Madrid, Marcial Pons, 2004).

Père, David - Forest, David, *L'arsenal répressif du* "phishing", en *Recueil Dalloz* (2006).

Piña Rochefort, Juan Ignacio, *Fraude de seguros, cuestiones penales y de técnica legislativa* (Santiago, Editorial Jurídica de Chile, 2006).

Politoff, Sergio - Matus, Jean Pierre - Ramírez, María Cecilia, *Lecciones de Derecho penal. Parte especial* (2ª edición, Santiago, Editorial Jurídica de Chile, 2004).

Quintero Olivares, Gonzalo - Carbonell Mateu, Juan Carlos y otros, *Esquemas de la Parte especial del Derecho Penal (I)* (Valencia, Tirant lo Blanch, 2011).

Quintero Olivares, Gonzalo a Valle Muñiz, José Manuel, *El delito de estafa: delimitación jurídico-penal con el fraude civil* (Barcelona, Bosch, 1987).

Real Academia Española, *Diccionario de la lengua española* (22ª edición, Madrid, Espasa Calpe, 2001).

Rivacoba y Rivacoba, Manuel, *Evolución histórica del Derecho penal chileno* (Valparaíso, Edeval, 1991).

Romeo Casabona, Carlos María - Sola Reche, Esteban - Sánchez Lázaro, Fernando y otros, *Informe sobre los nuevos instrumentos jurídicos en la lucha contra la delincuencia económica y tecnológica. Líneas de investigación y conclusiones*, en AA.VV., *Nuevos instrumentos jurídicos contra la delincuencia económica y tecnológica* (Granada, Comares, 2012).

Rosenbult Gorodinsky, Verónica, *Punibilidad y tratamiento jurisprudencia de las conductas de "phishing" y fraude informático*, en *Revista Jurídica del Ministerio Público*, 35 (2008).

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

Santana Vega, Dulce - Gómez Martín, Víctor, *Arts. 278-289*, en Corcoy Bidasolo, Mirentxu - Mir Puig, Santiago, *Comentarios al Código Penal. Reforma LO 5/2010* (Valencia, Tirant lo Blanch, 2011).

Scheechler, Christian, *El "childgrooming" en la legislación penal chilena: sobre los cambios al artículo 366 quáter del Código penal introducidos por la Ley N º 20.256*, en *Revista Chilena de Derecho y Ciencia Política*, 3 (2012) 1.

Schlack Muñoz, Andrés, *El concepto de patrimonio y su contenido en el delito de estafa*, en *Revista Chilena de Derecho*, 35 (2008) 2.

Seidl, Alexander - Fuchs, Katharina, *Die Strafbarkeit des* "phishing" *nach Inkrafttreten des 41. Strafrechtsänderungsgesetzes*, en *Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht*, 2 (2010).

Sieber, Ulrich, *El control de la complejidad en el ciberespacio global: a armonización*

de los delitos informáticos, en Delmas-Marty, Mireille - Pieth, Mark y otros (directores) y Morales, Marta (coordinadora), *Los caminos de la armonización penal* (Valencia, Tirant Lo Blanch, 2009).

Sieber, Ulrich, *Legal Aspects of Computer-Related Crime in the Information Society COMCRIME. Study prepared for the European Commission* (Santa Clara, University of Würzburg, 1998).

Silva, Hernán, *Las estafas: doctrina, jurisprudencia y derecho comparado* (2ª edición, Editorial Jurídica de Chile, Santiago, 2005).

Tröndle, Herbert - Fischer, Thomas, *Strafgesetzbuch und Nebengesetze* (53ª edición, München, Beck, 2006).

Vásquez Ruano, Trinidad, *Aproximación jurídica al spam desde la protección de datos de carácter personal*, en *Revista de Contratación Electrónica*, 33 (2002).

Velasco Núñez, Eloy, *Estafa informática y banda organizada. "phishing", "pharming", "smishing" y muleros,* en *La Ley Penal*, 49 (2008).

Velasco Núñez, Eloy, *Fraudes informáticos en red: del "phishing" al "pharming"*, en *La Ley Penal*, 37 (2007).

Vives Antón, Tomás Salvador - González Cussac, José Luis y otros, *Derecho penal. Parte especial* (3ª edición, Valencia, Tirant lo Blanch, 2010).

Vives Antón, Tomás Salvador González Cussac, José Luis, *De las defraudaciones*, en AA.VV., *Comentarios al Código Penal de 1995* (Valencia, Tirant lo Blanch, 1996), II.

Vives Antón, Tomás Salvador, *Fundamentos del sistema penal. Acción significativa y derechos constitucionales* (2ª edición, Valencia, Tirant lo Blanch, 2011).

Wilson, Deidre - Sperber, Dan, *La teoría de la relevancia,* en *Revista de Investigación Lingüística*, 7 (2004).

Yubero, Julio, *El engaño en el delito de estafa*: *doctrina y jurisprudencia* (2ª edición, Santiago, Cruz del Sur, 2010).