Pontificia Universidad Católica de Valparaíso
Facultad de Derecho
Escuela de Derecho

EL PHISHING COMO COMPORTAMIENTO PENALMENTE RELEVANTE

Catalina Fabiola Flores Cáceres
Profesor Guía: Dra. Laura Mayer Lux

Valparaíso, enero de 2017

ÍNDICE

INTRODUCCIÓN 3

I. DEFINICIÓN Y EVOLUCIÓN DEL *PHISHING*, ASÍ COMO SU DELIMITACIÓN RESPECTO DE OTRAS FIGURAS 5
a) ¿Qué es el phishing? 5
b) ¿Cómo surge el phishing? 6
c) ¿Quiénes cometen phishing? 7
d) ¿Cómo se comete el phishing? 8
e) Formas de ejecución del phishing 10
f) Delimitación respecto de otras figuras 11

II. NATURALEZA JURÍDICA DEL *PHISHING* 14
1. El phishing como parte de otras figuras delictivas 14
a)El phishing como acto preparatorio 19
b) El phishing como tentativa de delito en sentido amplio 25
2. El phishing como delito autónomo 36

III. JUICIO CRÍTICO 40

CONCLUSIONES 43

BIBLIOGRAFÍA

INTRODUCCIÓN

En la sociedad en que vivimos, a partir de la revolución industrial, la tecnología ha llegado a ocupar un lugar imprescindible en la cotidianeidad de las personas. Lo anteriormente descrito se inserta en un proceso de globalización –o, como algunos han planteado, de mundialización–, toda vez que existe una creciente comunicación e interdependencia a escala planetaria en aspectos económicos, culturales, tecnológicos y políticos. Este proceso de carácter dinámico en su aspecto tecnológico ha significado un gran avance en la conectividad humana, con la masificación de las tecnologías de la información y comunicación, facilitando la integración y el contacto de prácticas entre distintas partes del mundo.

En este contexto, se ha considerado que el Internet "es el corazón de un nuevo paradigma socio técnico que constituye, en realidad, la base material de nuestras vidas y de nuestras formas de relación, trabajo y comunicación. Lo que hace el Internet es procesar la virtualidad y transformarla en nuestra realidad, constituyendo la sociedad red, que es la sociedad en la que vivimos"[1].

Junto con ello, la criminalidad no queda al margen de tamaña influencia. Es así que descubre y aprovecha las potencialidades que este nuevo mundo ofrece. De esta manera, se ha dicho que "esta otra cara de la moneda de, por lo demás, tan potentes y versátiles tecnologías nos muestra, por consiguiente, su extraordinaria vulnerabilidad ante su utilización abusiva y con ello la aparición de un nuevo factor criminógeno de primera magnitud"[2].

Así, podríamos decir, provisionalmente, que con el término "cibercriminalidad" se alude a un "conjunto de actividades ilícitas cometidas al amparo del uso y abuso de las tecnologías de la información y la comunicación"[3]. En la actual sociedad de la información la denominada cibercriminalidad se presenta bajo las más variadas formas, a través de sistemas o redes informáticas de transmisión de datos por Internet, cuya complejidad operativa y constante transformación dificultan su persecución y, por lo mismo, aumentan su impunidad.

En este sentido, el Derecho Penal se ve enfrentado a una criminalidad especialmente poderosa y peligrosa desde variadas perspectivas, en vista de lo cual, pareciera que la mejor alternativa es otorgar una respuesta satisfactoria para brindar a lo menos certeza respecto de las situaciones delictivas que se han desarrollado en este ámbito que, todo parece indicar, irán en aumento.

---

[1] CASTELLS OLIVÁN, Manuel, *The Internet Galaxy: Reflections on the Internet, Business, and Society* (Oxford University Press, Oxford, 2003), p. 38.

[2] ROMEO CASABONA, Carlos, *De los delitos informáticos al cibercrimen. Una aproximación conceptual y político criminal*, en ROMEO CASABONA, Carlos (a cura di), *El Cibercrimen: nuevos retos jurídico-penales, nuevas propuestas jurídico criminales* (Granada, Comares, 2006), p. 2.

[3] OXMAN, Nicolás, *Estafas informáticas a través de Internet: acerca de la imputación penal del "phishing" y el "pharming"*, en *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso* 41 (2013) 2, p. 212.

Bajo esta perspectiva, la doctrina ha logrado identificar la comisión de ciertas figuras delictivas específicas constitutivas de cibercrimen, dentro de las que destaca como un comportamiento clave y, a estas alturas bastante frecuente, la figura del *phishing*, que será el elemento central de estudio en este trabajo.

Situados en este contexto, el objeto de esta memoria es dar cuenta, desde una mirada descriptiva, del comportamiento que se considerará constitutivo de *phishing* desde sus inicios, realizando asimismo un análisis de los principales elementos de esta figura.
Así, junto con delimitar aquello que entenderemos por *phishing*, al considerarse desde el punto de vista de este trabajo como un comportamiento penalmente relevante, se intentará determinar la naturaleza jurídica del *phishing* realizando un análisis completo de las posibilidades de subsunción del mismo.

Para lograr a cabalidad estos objetivos, este trabajo se estructura de la siguiente manera: Primero, se examinará el origen de la figura, tanto desde un ámbito conceptual como histórico. Segundo, se estudiarán también los elementos que le dan forma a este comportamiento, dando énfasis a aquellos que le otorgan características propias y únicas. Tercero, se delimitará la figura del *phishing* respecto de otras figuras que tienen lugar en el mismo ámbito, a saber, el *pharming* y el *hacking*, ya que la confusión entre unas y otras es bastante común. Cuarto, se analizarán las posibilidades de subsunción de la figura, sea un acto preparatorio, sea un acto de ejecución, sea un delito independiente.

I. DEFINICIÓN Y EVOLUCIÓN DEL PHISHING, ASÍ COMO SU DELIMITACIÓN RESPECTO DE OTRAS FIGURAS

Se debe tener presente desde un principio, que el *phishing* forma parte del cibercrimen. Este último, en su sentido tipológico[4], hace referencia a un comportamiento concreto que reúne un conjunto de características criminológicas relacionadas con el ciberespacio[5]. Asimismo, el cibercrimen puede ser entendido en términos amplios o restringidos.

Desde una concepción amplia, el cibercrimen puede ser definido como "cualquier comportamiento delictivo realizado en el ciberespacio, entendiendo además por el mismo el ámbito virtual de interacción y comunicación personal definido por el uso de las TIC, y dando cabida, por tanto, a conductas cuyo contenido ilícito es nuevo y se relaciona directamente con los nuevos intereses o bienes sociales existentes en el ciberespacio, así como también a comportamientos tradicionalmente ilícitos en los que únicamente cambia que ahora se llevan a cabo por medio de Internet"[6].

En cambio, desde una concepción restringida, constituirá cibercrimen solamente aquel comportamiento delictivo que se realiza en el ciberespacio "cuya esencia de injusto no podría haberse dado de ninguna forma fuera de él"[7].

Se debe señalar al respecto, que a lo largo de este trabajo se utilizará el término cibercrimen desde su concepción amplia, siendo cualquier delito en el que las Tecnologías de la Información y la Comunicación, en adelante TIC, juegan un rol determinante en su comisión. Las razones de esta elección podrán ser observadas finalizando el análisis de la figura que nos convoca: el *phishing.*

a) ¿Qué es el phishing?

En primer lugar, se debe analizar a grandes rasgos, qué es aquello que se ha denominado *phishing*. En este sentido, en las últimas décadas ha surgido una nueva forma de comportamiento, que generalmente consiste en el envío masivo de correos electrónicos, los cuales simulan una comunicación de carácter oficial, con el fin de obtener por parte de los receptores de estos mensajes, informaciones de carácter confidencial[8].

Este término ("*phishing"*), deriva de la evolución de la palabra *fishing*, aludiendo al intento de hacer que las potenciales víctimas muerdan un anzuelo. Asimismo, "los *hackers* frecuentemente reemplazan la letra 'f' con las letras 'ph', como raíz de la antigua

[4] Es posible distinguir al respecto dos sentidos del término cibercrimen; uno normativo, con el cual se hace referencia a una figura delictiva incluida en una ley determinada, permitiendo sancionar un conjunto de comportamientos; uno tipológico, el cual será explicado en las siguientes líneas. Al respecto véase MIRÓ, Fernando, *El Cibercrimen* (Madrid, Marcial Pons, 2012), pp. 39-40.
[5] *Ibidem*, p. 39.
[6] *Ibidem*, p. 42.
[7] *Ibidem*, p. 42.
[8] SÁNCHEZ BERNAL, Javier, *El bien jurídico protegido en el delito de estafa informática*, en *Cuadernos del Tomás* 1 (2009), p. 107.

forma de hacking telefónico conocida como *phreaking*"[9]. En este orden de ideas, tal como ocurre en la actividad pesquera en la cual se lanza una red, en el *phishing* se envía una gran cantidad de correos electrónicos, esperando que los usuarios no reconozcan la falsa apariencia de éstos y remitan los datos requeridos.

b) ¿Cómo surge el phishing?

Ahora bien, el origen de esta figura tiene relación con un comportamiento desarrollado respecto de una empresa estadounidense de servicios de Internet y medios, American Online (AOL), la cual, en respuesta a ciertos ataques que estaban llevando a cabo los *hackers* en su plataforma, creó una serie de barreras de seguridad. Esto tuvo como consecuencia que se buscaran nuevas formas de ataque, modificando su actuar hasta el desarrollo de la figura del *phishing*.

El objetivo principal de estos primeros ataques se centraba en obtener cuentas de usuario de la empresa, para así acceder a servicios de Internet de forma gratuita. En un principio, para lograr tal objetivo, los sujetos crearon cuentas de usuario en AOL, ingresando datos de identidad falsos y números de tarjetas de crédito que generaban a través de un sistema de algoritmos[10]. De esta manera, AOL consideraba legítimas estas cuentas y las activaba, dando pie para que los *hackers* las manipularan sin costo alguno. Sin embargo, tiempo después estas cuentas falsas quedaron al descubierto cuando la empresa realizó los cobros correspondientes, revelando que los datos ingresados no coincidían con los de los verdaderos dueños de las tarjetas.

Como ya se mencionó, American Online tomó medidas activas para prevenir los ataques anteriormente descritos. De manera que realizaba una verificación inmediata de la legitimidad de los datos entregados por los usuarios al momento de la creación de las cuentas[11]. Como es posible observar, el sistema que hasta ese momento habían ideado los *hackers* para obtener las cuentas se tornó ineficaz.

Por ello, su nuevo objetivo fue obtener datos verdaderos pertenecientes a usuarios ya registrados en las plataformas de la empresa, pues de esta forma la barrera impuesta por AOL no surtiría efectos. Ahora bien, para cumplir con estos nuevos objetivos, los sujetos comenzaron a contactar a los verdaderos usuarios de la empresa, haciéndose pasar por empleados de AOL. Esta comunicación normalmente era iniciada por medio de un correo electrónico o a través del servicio de mensajería instantánea de la misma institución[12]. Por medio de este acto, se le solicitaba a los usuarios que remitieran cierta información,

[9] MIRÓ, Fernando, cit. (n. 4), p. 72.
[10] SÁNCHEZ BERNAL, Javier, cit. (n. 8), p. 107.
[11] JAKOBSSON, Markus; MYERS, Steven, *Phishing and Countermesaures:Understanding the Increasing Problem of Electronic Identity Theft* (New Jersey, Wiley, 2007), p. 2.
[12] NYKODYM, Nick, KAHLE-PIASECKI, Lisa, ARISS, Sonny, TOUSSAINT, Tracey, *Cibercrime and Business: How to not Get Caught by the Online Phisherman*, en *Journal of International Commercial Law and Technology* 5 (2010) 4, p. 253.

principalmente contraseñas, con frecuencia bajo la excusa de otorgarle mayor seguridad al servicio[13].

Las conductas recientemente descritas son probablemente los ejemplos más tempranos de *phishing*, los que fueron nombrados por vez primera en el grupo de noticias de *hackers* <<alt.2600>>[14], en referencia a la búsqueda de nuevas formas de conseguir cuentas de AOL distintas a la generación automática de números de tarjetas de crédito.
Cabe destacar que "estas cuentas robadas fueron denominadas *phish* y se convirtieron a partir de 1997 en habitual moneda de cambio entre *hackers*, de modo tal que ciertas aplicaciones o juegos podían ser intercambiados por un determinado número de cuentas de AOL"[15].

Debido al éxito de estos ataques, los *phishers* han evolucionado gradualmente y junto con ello, también las técnicas que ellos emplean. Representación de lo mismo es que estos sujetos dejaron de considerar como víctimas solamente a clientes de la empresa American Online, y comenzaron a dirigir sus ataques a cualquier usuario de Internet. Asimismo, el *phisher* ya no solo se hizo pasar por un agente de AOL, al contrario, trabajó de forma activa para imitar un sinnúmero de entidades dedicadas al comercio online e instituciones financieras.

En este sentido, el objetivo de la actividad de estos sujetos se ha tornado cada vez más ambicioso, por lo que ya no resulta suficiente utilizar como propia una cuenta online de otro usuario para acceder a servicios de Internet de forma gratuita; los *phishers* más bien se centran en obtener números de tarjetas de crédito reales, junto con la respectiva información confidencial de las cuentas[16].

c) ¿Quiénes cometen phishing?

Es parte de la evolución del *phishing* el desarrollo de labores especializadas por los sujetos que lo practican, los cuales pueden llegar a ejecutar un trabajo en equipo, de manera que el resultado sea el más eficiente. En vista de lo anterior, los expertos han diferenciado tres categorías, a saber, mensajeros, recolectores y cajeros.

En primer lugar, se encuentran los mensajeros o *mailers*, los cuales están encargados principalmente de enviar grandes cantidades de correos electrónicos con contenido engañoso[17].

---

[13] JAKOBSSON, Markus; MYERS, Steven, cit. (n. 11), p. 2.
[14] Alt.2600 es una revista técnica fundada en 1984 por "Emmanuel Goldstein", quien a su vez también es su editor. La publicación, llamada "la biblia del hacker", se ha centrado en la exploración tecnológica y el saber hacer, exponiendo el gobierno y las fechorías corporativas. 2600: El Hacker Quarterly ha estado involucrado continuamente en los debates legales, éticos y técnicos sobre la piratería informática. Junto con ello, es también la organizadora de conferencias "Hackers on Planet Earth" (H.O.P.E), que se realizan cada dos años en la ciudad de New York. Véase NIARCOS, Nicolas, *The Newyorker*. Disponible en http://www.newyorker.com/tech/elements/print-magazine-hackers
[15] MIRÓ, Fernando, cit. (n. 4), p. 73.
[16] JAKOBSSON, Markus; MYERS, Steven, cit. (n. 11), p. 3.
[17] *Ibidem*, p. 3.

En segundo lugar, están los recolectores o *collectors*, cuya principal función es configurar los sitios web falsos a los que son dirigidos los receptores de los correos electrónicos enviados por los mensajeros. De estas páginas web falsas se obtienen una serie de datos, tales como la identificación de usuarios, contraseñas, números de tarjetas de crédito, etc.[18]

En tercer lugar, surgen los cajeros o *cashers*, quienes reciben esta información conseguida por los recolectores y la utilizan. Son variados los usos que puede darse a esta información confidencial, partiendo por la creación de tarjetas de crédito para obtener dinero, pasando por la transferencias de fondos desde una cuenta a otra o la compra de productos online, hasta llegar incluso a la venta misma de esta información a otros[19].

Las transferencias pueden beneficiar al *phisher* de variadas formas, puede simplemente enviarse el dinero a su cuenta. Pero también esas transferencias podrían tener como objeto el pago de deudas del mismo *phisher*. Así también, el *phisher* podría comprar cosas para sí, con cargo al patrimonio de la víctima.

No obstante la anterior distinción, a lo largo de este trabajo se utilizará desde una perspectiva amplia el término "*phisher*" para aludir de forma general al sujeto que realiza el ataque como *mailer*, *collector* o *casher*.

d) ¿Cómo se comete el phishing?

Son variadas las herramientas utilizadas por los *phishers* para llevar a cabo con éxito sus ataques. Es ya de uso generalizado dentro de los entendidos en temáticas de cibercrimen referirse a ellas como la ingeniería social y los subterfugios técnicos[20].

La primera, esto es, la ingeniería social, se refiere a todas las actividades tendientes a obtener la confianza de la víctima, en las que se entrega una serie de razones plausibles o incentivos idóneos en orden a que el receptor se forme la convicción de que el mensaje es verdadero y, por ende, entregue sin reservas sus datos[21]. Algunas de las ingenierías sociales más destacables son las "actualizaciones de seguridad". A modo de ejemplo, las supuestas empresas proveedoras de servicios online comunican a sus usuarios que se está introduciendo un nuevo servicio para aumentar la seguridad del consumidor y, de esta manera, evitar fraudes. Junto con ello, para activar el servicio es necesario que el usuario autentifique cierta información con lo que el *phisher* logra su cometido. Asimismo, otra clara manifestación de este mecanismo se encuentra con motivo de una supuesta "información de cuenta incompleta", situación en la cual se les dice a los usuarios que los servidores poseen información obsoleta o incluso, que hay ciertos datos que se han

[18] MIRÓ, Fernando, cit. (n. 4), p. 74.
[19] JAKOBSSON, Markus; MYERS, Steven, cit. (n. 11), pp. 3-4.
[20] MIRÓ, Fernando, cit. (n. 4), p. 72.
[21] SÁNCHEZ BERNAL, Javier, cit. (n. 8), p. 106.

perdido, por lo que para mantener el servicio es necesario que ingresen al sitio web indicado y actualicen la información solicitada[22].

La segunda, o sea, los subterfugios técnicos, alude al uso del conocimiento científico, especialmente de la informática, cuyo objetivo principal es lograr con mayor efectividad el convencimiento de la víctima del ataque de que las comunicaciones entabladas con los *phishers* son verdaderas. El subterfugio técnico más evidente, pero al mismo tiempo esencial, es la utilización de logos e imágenes corporativas que imitan a la perfección los originales, cuya inclusión reporta para la víctima una falsa sensación de seguridad. Igualmente surgen los denominados *bot-net*[23], de los cuales se valen los *phishers* para el envío de grandes cantidades de correos sin que sea posible rastrearlos de vuelta, favoreciendo el anonimato del ataque[24].

Ahora bien, con miras a obtener un estudio más completo y claro acerca de cómo se lleva a cabo el *phishing*, algunos autores han optado por dividirlo en tres componentes o etapas.
1. Un mensaje considerado como "señuelo" (*the lure)*, el cual se envía principalmente por correo electrónico con el método del *spam* a un gran número de destinatarios. La principal característica de este mensaje es que aparenta ser proveniente de alguna entidad verdadera con presencia en Internet.

Dentro de las estrategias de engaño más claras podemos encontrar, como se indicó anteriormente, el caso de mensajes que solicitan actualizaciones de seguridad de cuenta, o situaciones en que por razones de mantenimiento se pide completar ciertas informaciones de cuenta, o incluso ciertas proposiciones relacionadas con futuros beneficios o incentivos financieros, valiéndose de la expectativa de ganancia del receptor para incitarlo a entregar información delicada que en otras circunstancias no habría proporcionado[25].

En nuestro país, en los últimos años, se ha hecho cada vez más frecuente la estrategia en la que se piden datos para la actualización de la seguridad de las cuentas bancarias, más específicamente, la solicitud de la tercera clave de seguridad de las cuentas corrientes.

---

[22] Se mencionan como los escenarios más comunes; *Security Update*, *Incomplete Account Information*, *Financial Incentive*, False Account Updates. Con más detalle en JAKOBSSON, Markus; MYERS, Steven, cit. (n. 11), p. 16.
[23] Se debe entender en primer lugar, que un "*bot*" es una clase de programa malicioso que permite al atacante tomar el control de un equipo. De esta forma, las máquinas infectadas realizan lo que el *phisher* ordene, comportándose como un "robot" o "zombie". El gran número de máquinas infectadas por el "*bot*" forman una red denominada "*robot network"*, cuya abreviación es el referido término "*bot-net*". La característica principal de esta técnica es que posee un solo centro de comando y control a distancia, que se encuentra a cargo del *phisher*, desde el cual se ordena el envío masivo de correos electrónicos proveyendo un nivel de indeterminación y disgregación del que sería el emisor del mensaje. Lo anterior tiene como consecuencia el que se torne imposible rastrear el origen del mensaje. Con extremo detalle, véase LEE, Wenke, WANG, Cliff, DAGON, David, *Botnet Detection: Countering the Largest Security Threat* (New York, Springer, 2008), pp.1-2. Así también JAKOBSSON, Markus; MYERS, Steven, cit. (n. 11), p. 17.
[24] JAKOBSSON, Markus; MYERS, Steven, cit. (n. 11), pp. 12-18.
[25] MIRÓ, Fernando, cit. (n. 4), p. 74.

2. Una vez que las posibles víctimas reciben el mensaje, el siguiente paso que tiene lugar es la efectiva interacción entre el receptor y el *phisher*. Se debe tener presente que si bien los mensajes son remitidos a una gran cantidad de usuarios, es habitual que solo algunos de ellos consideren realmente su contenido, es por esto que estos primeros mensajes se consideran solo "señuelos". Así las cosas, el propósito del segundo elemento es actuar como una especie de "gancho" ("*the hook*"), para que la propia víctima reenvíe sus datos por medio del mismo correo electrónico o que se dirija a un sitio web que normalmente imita de manera casi idéntica la apariencia de una institución legítima[26], inspirando confianza en el receptor. En este sentido, los *phishers* se han concentrado en la construcción de páginas web, cuya falsedad es prácticamente imperceptible, utilizando para ello diversas técnicas. Destaca entre ellas, por un lado, el registro de nombres de dominio muy similares[27], verbigracia *aliexpress-login.com, ebay.com.site.com* en contraposición a los verdaderos *aliexpress.com y ebay.com* respectivamente. Por otro lado, es la regla general el uso de imágenes y logos institucionales de forma llamativa para inspirar la seguridad y carácter verdadero del sitio[28].

En caso de que la víctima se sitúe en la web programada por el *phisher*, se le solicita que entregue información sensible o también puede ocurrir que se instale sin su conocimiento un *malware*. Son ejemplos de esta información confidencial requerida los nombres de usuario, contraseñas, números de cuenta, números de tarjetas de crédito, etc.

En suma, este segundo componente se encarga principalmente de convencer a la víctima de la legitimidad del sitio y alentarla para proveer la información sensible que le es solicitada.

3. Finalmente, algunos autores agregan un tercer elemento, el cual se centra en la utilización de los datos suministrados por las víctimas para diversos propósitos. El término descriptivo original para esta fase, "*the catch*"[29], alude precisamente al acto de tomar la información y hacer uso de ella, pudiendo ser en ciertos casos de forma directa por parte del *phisher*, como por ejemplo, realizando transferencias electrónicas a cuentas propias o utilizando los datos para subastas *online*. Sin embargo, en variadas ocasiones los datos recolectados terminan siendo remitidos a terceros producto de una venta en el mercado "negro".

e) Formas de ejecución del phishing

Como ya se ha descrito anteriormente, la forma más tradicional y común de *phishing* es a través del envío masivo de correos electrónicos utilizando la técnica del *spam*, que en otras palabras alude al "correo electrónico no solicitado que suele enviarse a numerosas

[26] Si bien como se observará más adelante la creación de sitios web falsos es característica y esencial en la figura del *pharming*, no parece ser exclusiva de esta figura ni tampoco incompatible con aquello que conforma el *phishing*.
[27] Se hace referencia a ello bajo el término "subdominios", en SÁNCHEZ BERNAL, Javier, cit. (n. 8), p. 107.
[28] MIRÓ, Fernando, cit. (n. 4), p. 75.
[29] JAKOBSSON, Markus; MYERS, Steven, cit. (n. 11), pp. 5-6.

direcciones a través de una dirección electrónica de las ofrecidas por servicios de correo gratuito o desde un sistema informático infectado"[30].

En estos mensajes se hace uso además de la imagen corporativa de una institución con presencia en Internet, solicitando que se envíe a una dirección de correo electrónico similar a la de la entidad, la información confidencial requerida.[31]

Se añaden a lo anterior formas más elaboradas de la figura, como es el caso del "*spear phishing* o <<pesca con arpón>>, en la que en lugar de dirigirse a objetivos indiscriminados, se buscan clientes de entidades bancarias[32] u otro tipo de organizaciones concretas"[33]. A modo explicativo, si una persona realiza todas sus actividades bancarias con Banco Estado, en caso de recibir un mensaje imitando la imagen de Banco de Chile, este será fácilmente reconocido como falso, pudiendo alertar a la institución respectiva. En cambio, si la misma persona recibe un mensaje, esta vez con la imagen de Banco Estado, las probabilidades de que el ataque sea exitoso son mucho más altas que en las otras modalidades. Esta es la lógica que opera bajo el *spear phishing.*

Por otra parte, como ya se ha mencionado, puede que el *phishing* actúe basado en un *malware*, el cual puede presentarse de diversas formas. Una de ellas, cuyas primeras manifestaciones se registran desde el año 2000, son los denominados *keyloggers*, un programa cuya función básicamente es "registrar[34] todo lo que los usuarios teclean en su ordenador"[35]. Otra forma que podemos encontrar son los llamados *screenloggers*, un programa que actúa bajo la misma lógica que los *keyloggers*, con la diferencia de que en este caso aquello que se registra son los contenidos de la pantalla del ordenador[36].
Asimismo, puede ocurrir que tenga lugar un programa espía o *spyware*, el cual es capaz de permanecer por mucho tiempo oculto en el sistema y se activa cuando el usuario accede a las páginas de bancos u otras entidades, capturando las claves de acceso o incluso capturando las pantallas para conocer el estado de las cuentas corrientes[37]. El objeto de estos es el envío a un lugar exterior, que generalmente será el ordenador del atacante, de los datos del sistema en el que fueron instalados sin el conocimiento del usuario[38].

f) Delimitación respecto de otras figuras

[30] MIRÓ, Fernando, cit. (n. 4), p. 66.
[31] MIRÓ, Fernando, cit. (n. 4), p. 76.
[32] Se crearía el señuelo de acuerdo a la víctima. Véase SÁNCHEZ BERNAL, Javier, cit. (n. 8), p. 107.
[33] MIRÓ, Fernando, cit. (n. 4), p. 76.
[34] El *keylogger* monitorea al atacado registrando la actividad que realiza a través del teclado y del mouse. También podría ocurrir que este *malware* quede instalado en la barra de búsqueda del navegador, pudiendo detectar los cambios de URL creando luego un listado con los sitios de interés para el *phisher*. Véase JAKOBSSON, Markus; MYERS, Steven, cit. (n. 11), p. 34.
[35] FERNÁNDEZ TERUELO, Javier, *Derecho penal e internet* (Volladolid, Editorial Lex Nova, 2011), p. 37.
[36] MIRÓ, Fernando, cit. (n. 4), p. 77.
[37] FLORES, Fátima, *Respuesta penal al denominado robo de identidad en las conductas de phishing bancario*, en *Estudios penales y criminológicos* 34 (2014), p. 305.
[38] FERNÁNDEZ TERUELO, Javier, *Derecho penal*, cit. (n. 35), p. 36.

Junto con ello, antes de continuar con el análisis referido estrictamente a la figura del *phishing*, se torna necesario referirse también a otras figuras insertas en el mismo ámbito del cibercrimen, a saber, el *pharming* y el *hacking*, las cuales tienden a ser confundidas fácilmente con la figura en estudio.

Con el fin de entender con mayor precisión cómo actúa el *pharming*, se debe tener presente que los ordenadores no se conectan a las redes por medio de un nombre o URL (www.bancochile.cl), sino que lo hacen gracias a una convención informática numérica denominada dirección IP. Simultáneamente, existe una estructura que realiza el trabajo de traducción de esa URL y su dirección IP, llamada *Domain Name Server*[39] o DNS. La razón que fundamenta la utilización de una URL es que facilita el uso de las redes para los usuarios, prefiriendo el empleo de letras de manera lógica por sobre una serie de números.

"Los servidores DNS son los encargados de conducir a los usuarios a la página que desean ver. Pero, a través de esta acción, quien pretende defraudar consigue que las páginas visitadas no se correspondan con las auténticas sino con otras creadas para recabar datos confidenciales, sobre todo relacionadas con la banca *on-line*"[40].

La referida manipulación se logra generalmente a través de un *malware*, específicamente por medio de los *host file poisoning*, cuyo resultado es que se alteren los archivos de DNS[41].

Así las cosas, el ataque funciona de la siguiente manera[42]: Primero, el usuario digita la dirección URL de la página que quiere ver en la barra de búsqueda, que comúnmente corresponde a la del banco donde realiza sus transacciones bancarias, v.gr. www.bancochile.cl. Luego, la solicitud pasa al DNS, el cual convertirá la URL en una serie de números que conforman la dirección IP (por ejemplo, 210.10.10.3). En un escenario normal, la barra de búsqueda se conectará con la autentificación del sitio del banco, sin embargo, en el *pharming* el atacante modifica las conexiones de datos que posee el DNS. En el ejemplo dado, la URL www.bancochile.cl remitirá a otra IP, 230.10.10.3, dirección que corresponde a un sitio web construido por el atacante. De esta forma, el cliente piensa que está interactuando con la verdadera página de la entidad, pues así lo indica la dirección en la barra de búsqueda, cuando en realidad está conectado con la web del atacante. En este sentido, el *pharming* consiste 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"[43].

Bajo este respecto, el *pharming* se diferencia del *phishing* en cuanto este último tiene lugar a partir de una comunicación con apariencia de verdadera, en virtud de la cual se

[39] FLORES, Fátima, *Respuesta*, cit. (n. 37), p. 304.
[40] FERNÁNDEZ TERUELO, Javier, *Derecho* penal, cit. (n. 35), p. 38.
[41] MIRÓ, Fernando, cit. (n. 4), p. 77.
[42] SRIVASTAVA, Tushar, *Phishing and Pharming- The deadly two* (Boston, Sans Institute, 2007), p. 18.
[43] OXMAN, Nicolás, cit. (n. 3), p. 217.

solicita al receptor que entregue información confidencial. Asimismo, la víctima del ataque entrega sus datos personales al *phisher*, con la convicción de que lo hace por razones legítimas a la verdadera institución.
En tanto, en el *pharming* la víctima no actúa en respuesta de ninguna comunicación sostenida con el *phisher*, sino que se desenvuelve con completa normalidad en su navegador web, cuyo DNS se encuentra alterado por los *host file poisoning*. En esta misma lógica, si bien es la víctima quien entrega la información al atacante, lo hace sin estar consciente de que un tercero está accediendo a tales datos. En el *pharming* tampoco es necesario contactar a las víctimas de manera individual para esperar luego una respuesta consciente de parte de ellas, sino que la manipulación se lleva a efecto de todas maneras, aun cuando el usuario haya digitado de manera correcta la dirección que pretende visitar.

Por otra parte, se encuentra la figura del *hacking*, la cual consiste principalmente en "acceder de forma no autorizada o no consentida a bases de datos o a sistemas informáticos ajenos mediante la vulneración de puertas lógicas o *passwords*"[44]. Lo anterior se configura de manera tal que potencialmente el *hacker* tiene al alcance todo tipo de información que esté presente en el sistema de que se trate.

Cabe destacar al respecto, que esta figura se trata siempre de un acceso remoto, es decir, que se lleva a cabo a distancia sin tener contacto material con el sistema mismo, actuando comúnmente por medio de las redes de Internet. Ahora bien, este acceso a los sistemas informáticos "se puede llevar a cabo de muy distintas formas, si bien generalmente, el modo de proceder consiste en la búsqueda de vulnerabilidades en los sistemas informáticos derivadas de una deficiente programación, de un cambio tecnológico que hace obsoleta la formulación binaria existente, o incluso, en la búsqueda y uso de las puertas que involuntariamente el propio titular del sistema informático o cualquiera de los múltiples sujetos que interaccionan con él pueden haber dejado abiertas"[45].

En vista de ello, parte de la doctrina ha optado por distinguir entre el *hacking* puro o directo y aquel denominado *cracking*. En cuanto al primero, este consiste simplemente en "acceder de manera indebida o sin autorización a un sistema o a los datos allí contenidos, con el fin de obtener una satisfacción de carácter intelectual por el desciframiento de los códigos de acceso o *passwords*, no causando daños inmediatos y tangibles en la víctima, o bien por la mera voluntad de curiosear o divertirse de su autor"[46]. Es decir, se trata de actos cuyo objetivo principal consiste en lograr ingresar al sistema, pero una vez que se consigue este propósito no se efectúa una alteración del mismo. Por su parte, en la forma denominada *cracking* se "accede al sistema para realizar cualquier tipo de daño al sistema, a los elementos que él contiene, o a su titular al adquirir, eliminar o modificar información del mismo"[47].

---

[44] RUEDA, María, *Cuestiones político-criminales sobre las conductas de hacking*, en *Derecho penal contemporáneo: Revista Internacional* 28 (2009), p. 152.
[45] MIRÓ, Fernando, cit. (n. 4), p. 54.
[46] HUERTA, Marcelo, *Los delitos de hacking en sus diversas manifestaciones*, en *Revista de Derecho Público de la Agrupación de Abogados de la Contraloría General* 6 (2001), p. 83.
[47] MIRÓ, Fernando, cit. (n. 4), p. 54.

Así las cosas, es posible diferenciarlo ampliamente de la conducta de *phishing*, toda vez que el *hacking* se trata de una actividad en que es el mismo sujeto atacante el que realiza todos los actos tendientes a lograr su objetivo final, cual es ingresar al sistema informático de la víctima del ataque. En este mismo sentido, respecto del *hacking* es casi nula la interacción que se da entre aquel que será atacado y el *hacker*.

Asimismo, los objetivos de uno y otro difieren, por cuanto tratándose del *phishing* los actos que lleva a cabo el *phisher* (envío de correos electrónicos, creación de páginas web) son todos tendientes a lograr la obtención de datos de carácter confidencial del receptor de un mensaje, lo cual no pareciera ser la principal finalidad del *hacking*, sea que se trate del *hacking* puro, con el mero acceso al sistema, sea que se trate del *cracking*, en cuanto al acceso y alteración (maliciosa) del mismo.

De esta forma, se ha podido describir el *phishing* como conducta específica y diferenciable de otras existentes en el mismo ámbito, con características propias y únicas, que hacen meritorio su estudio en particular. A partir del análisis efectuado es posible definir el *phishing* como aquel comportamiento por el que un sujeto emplea la ingeniería social o subterfugios técnicos para engañar a otro, por medio de comunicaciones aparentemente verdaderas, logrando que este último le remita información de carácter confidencial. Pues bien, con miras a lograr un análisis más acabado del *phishing*, cabe preguntarse cuál es la naturaleza jurídica de la conducta ya descrita.

II. NATURALEZA JURÍDICA DEL PHISHING

1. El *phishing* como parte de otras figuras delictivas

Ahora bien, con miras a responder la interrogante acerca de la naturaleza jurídica del *phishing*, se debe tener presente que nos situamos en el ámbito de aquello que se ha denominado *iter criminis*, término con el cual se alude a la progresión de etapas sucesivas que conforman el proceso de ejecución de un delito.

Así, se debe mencionar que primero el sujeto idea el hecho punible, de modo que se representa intelectualmente la posibilidad de realización del mismo. Luego, si su voluntad acoge aquello que ha discurrido, el sujeto resuelve cometerlo, disponiéndose a planificar su conducta. Posteriormente, se dirige a preparar la ejecución del hecho punible, para lo cual ordena los medios e instrumentos para asegurar su éxito. Solo una vez que se encuentra en este punto se orientará a verificar la acción típica, o si se tratara de delitos de resultado, a causar el evento típico[48]. Culmina este desarrollo con la consumación del hecho típico, es decir, con la realización completa de este. Al respecto, la doctrina ha entendido que el delito se encuentra consumado en aquellos casos en que el hecho concreto corresponde exactamente a la descripción abstracta que está contenida en

[48] CURY URZÚA, Enrique, *Derecho Penal Parte General* (Santiago, Ediciones UC, 2011), p. 549.

el tipo que la ley señala[49]. Asimismo, "hay quienes hablan también de delito agotado, refiriéndose a aquel momento del desarrollo del delito en que se han producido todas las consecuencias del hecho delictuoso y en que el sujeto activo, por consiguiente, no sólo ha dado cima al hecho típico, sino ha logrado, además, obtener todos los efectos ilícitos que mediante él se proponía conseguir"[50].

Bajo esta lógica, es posible distinguir en la realización del hecho punible dos fases: una interna o psicológica y otra externa o material.
1.La fase interna corresponde a aquella que se desarrolla en la *psiquis* del sujeto, y "consiste en fenómenos psicológicos del sujeto no trascendentes al exterior ni perceptibles por extraños"[51]. Generalmente, aquí tiene lugar una ideación del plan delictivo, seguido de una deliberación acerca de éste, ponderando las consiguientes ventajas e inconvenientes que pudieran conllevar la realización del hecho punible[52], sucedida por la resolución de realizarlo[53]. Resulta conveniente decir en todo caso, que "los pensamientos y voliciones criminales carecen de significación si no se manifiestan externamente"[54], ello debido a que en este período tiene aplicación el principio *cogitationem poena nemo patitur,* lo que implica que las ideas o pensamientos no pueden ser constitutivas de delito, sino que solo pueden serlo las conductas[55]. Debido a lo anterior, "suele decirse que esta etapa 'no interesa al derecho penal' lo cual entendido literalmente sería un grave error"[56]. En efecto, si bien la fase interna a falta de exteriorización queda al margen del derecho penal, con posterioridad a su ocurrencia cobra gran importancia en aspectos especialmente determinantes dentro de la teoría del delito como lo es, por ejemplo, la teoría de la culpabilidad[57].

2. En la fase externa, en tanto, el sujeto una vez que ha resuelto la comisión del hecho punible, se dirige a realizar lo necesario para cumplir con su fin, proyectando de esta forma su propósito de delinquir en la exterioridad. Existe, por tanto, un traslado del dominio psicológico en el que se centraba la fase interna, hacia una "materialización de la voluntad criminal"[58]. Así, "algunos de los actos de que se vale para cumplirlo están distantes de la consumación misma, pero gradualmente se va acercando a ésta con actos mas próximos y directos hasta que llega, finalmente a su meta"[59].

---

[49] Véase ampliamente en POLITOFF LIFSCHITZ, Sergio, *Los Actos preparatorios del delito tentativa y frustración: Estudio de dogmática penal y de derecho penal comparado* (Santiago, Editorial Jurídica de Chile, 1999), pp. 13-16.
[50] NOVOA, Eduardo, *Curso de Derecho Penal Chileno Parte General* (Santiago, Editorial Jurídica de Chile, 2005), p. 106.
[51] NOVOA, Eduardo, cit. (n. 50), p. 111.
[52] *Ibidem*, p. 111.
[53] ETCHEBERRY ORTHUSTEGUY, Alfredo, *Derecho Penal Parte General* (Santiago, Editorial Jurídica de Chile, 1998), p. 52.
[54] LABATUT GLENA, Gustavo, *Derecho penal* (Santiago, Editorial Jurídica de Chile, 1990) I, p. 179.
[55] Así también GARRIDO MONTT, Mario, *Derecho Penal Parte General* (Santiago, Editorial Jurídica de Chile, 2003) p. 261.
[56] ETCHEBERRY ORTHUSTEGUY, Alfredo, cit. (n. 53), p. 52.
[57] *Ibidem*, p. 52.
[58] LABATUT GLENA, Gustavo, cit. (n. 54), p. 180.
[59] NOVOA, Eduardo, cit. (n. 50), p. 111.

Dentro de la fase externa se distingue una etapa de preparación y otra se ejecución. La primera, se inicia en el momento en que el individuo manifiesta de forma externa su voluntad delictiva por la realización de actos materiales encaminados a favorecer la realización del hecho. La segunda, tiene como principal característica "el aprovechamiento de los medios obtenidos en la etapa de preparación para el cumplimiento del plan ejecutivo del hecho"[60]. Por consiguiente, es posible encontrar en la fase externa tanto actos preparatorios como actos de ejecución.

Cabe preguntarse en este punto, teniendo en cuenta la impunidad de la fase puramente interna, si la fase externa, sea en su totalidad, sea en parte, es sancionable penalmente. Cobra relevancia al respecto la distinción entre actos preparatorios y actos de ejecución, pues "la regla general, defendida por los clásicos, es la impunidad de los actos preparatorios, que están todavía muy alejados de la realización completa del evento"[61].

En este orden de ideas, se torna necesario establecer un límite a fin de precisar desde qué momento será punible la conducta que se dirigirá a la consumación del hecho típico. Ciertamente, existe acuerdo en cuanto a que no cualquier exteriorización del propósito criminal debe ser sancionada, pero a pesar de ello, las posturas sobre la implantación de estas fronteras son muy dispares[62].
Cobra relevancia en este punto, el enfoque impuesto con la promulgación del Código Penal Francés, "conforme al cual son punibles sólo aquellos actos del '*iter criminis*' que constituyen un principio de ejecución del delito (*commencement d'execution)"*[63]. Surge en este sentido, como problema fundamental, la delimitación entre los actos preparatorios y actos de ejecución, a lo que la doctrina ha intentado arduamente darle una solución, desarrollando una serie de teorías en orden a lograr un criterio satisfactorio.

Para ello, resulta útil la distinción de estas teorías entre objetivas y subjetivas. Para las objetivas, el carácter ejecutivo de los actos se otorga con prescindencia del propósito que perseguía el sujeto, por lo que se contempla el acto en sí mismo en cuanto acontecimiento externo[64]. Para las teorías subjetivas, la diferencia entre acto preparatorios y de ejecución se logra teniendo en consideración la finalidad que el sujeto tenía al momento de efectuarlo[65]. Se debe advertir, en todo caso, que estas teorías si bien se asimilan en cuanto a la referencia a elementos de carácter psíquico, difieren de forma significativa respecto de los criterios utilizados para marcar el límite de una actuación ejecutiva punible[66].

---

[60] GARRIDO MONTT, Mario, cit. (n. 55), p. 261.
[61] ETCHEBERRY ORTHUSTEGUY, Alfredo, cit. (n. 53), p. 53.
[62] Más profundamente en CURY URZÚA, Enrique, *Tentativa y delito frustrado: el proceso ejecutivo del delito* (Santiago, Editorial Jurídica de Chile, 1977), p. 28.
[63] *Ibidem*, p. 28.
[64] A su vez, a partir de las teorías objetivas se ha diferenciado entre teorías propias e impropias. "Las primeras son aquellas para las que sólo es ejecutivo el acto típico; las segundas, en cambio, admiten que algunos actos se consideren ejecutivos aunque no pertenezcan todavía, al proceso descrito por el esquema rector del delito correspondiente". Véase CURY URZÚA, Enrique, *Derecho Penal*, cit. (n. 48), pp. 552-553.
[65] GARRIDO MONTT, Mario, cit. (n. 55), p. 272.
[66] De igual forma, estas teorías admiten distinción entre las teorías extremas y limitadas. En efecto, las primeras "son concepciones para las cuales la tentativa comienza con la exteriorización de una voluntad cuya manifestación reúne ciertas características que fundamentan su punibilidad". En cambio, las segundas "consideran que sólo puede castigarse a este título aquella conducta que ha dado principio a la ejecución

Dentro de las teorías objetivas propias[67] destaca la teoría formal de Beling, que plantea que se debe llevar a cabo un análisis a nivel de tipicidad, teniendo especial relevancia el núcleo del tipo, por cuanto se decide si la conducta es posible de ser expresada por el verbo que describe la acción típica. En este sentido, no es posible obtener una fórmula de carácter general aplicable a la totalidad de las figuras delictivas, sino que dependerá de cada tipo en específico[68]. En esta misma línea, el examen de la relación entre el acto efectuado y el tipo se realiza en abstracto. Esto quiere decir que aquello que constituye un comienzo de ejecución para un delito en particular, lo es para todos los casos del referido delito[69].

Así las cosas, si con el acto efectuado aún no se realiza la acción descrita por el tipo, este será solo preparatorio, a pesar de que pueda encontrarse dirigido subjetivamente a la consumación de un delito[70].

Se debe mencionar asimismo la teoría formal material o también denominada teoría mixta, según la cual, el acto realizado será considerado ejecutivo si se efectúa una parte de aquello que se encuentra descrito en el tipo. Sin embargo, esta teoría se distingue de la concepción meramente formal en cuanto al criterio utilizado para determinar el contenido del hecho típico, pues recurre a la descripción típica en conjunto con complementos materiales[71]. Con este último término se extiende la noción de acto ejecutivo a "aquellos que sin ser tales, por su necesaria unión con la acción típica, aparecían según la concepción natural de la actividad, como incorporados a esa acción"[72]. Con frecuencia, se menciona como complemento natural a la figura del peligro, y en tal caso, un acto será ejecutivo si el bien jurídico tutelado se encuentra en una situación de peligro[73].

Por su parte, en cuanto a las teorías objetivas impropias, destaca particularmente la llamada teoría pragmática de Carrara. Este autor en su primer período –pues más tarde abandonaría esta teoría– distinguió los actos según su naturaleza, pudiendo ser unívocos o equívocos. Son actos unívocos, y consecuentemente actos ejecutivos, aquellos que "sólo pueden entenderse dirigidos a la perpetración del delito"[74], en tanto se encaminan

---

del hecho descrito por el tipo del delito consumado pero, para determinar si tal cosa ha ocurrido, se refieren a propósito del autor, o a la forma en que se presentó la situación y al modo que, consiguientemente, planificó la acción, o a todos esos factores conjuntamente". Así lo plantea en CURY URZÚA, Enrique, *Tentativa*, cit. (n. 62), p. 56.

[67] Destaca adicionalmente Cury la existencia de una teoría escéptica, la cual no obstante plantear como necesario distinguir entre actos preparatorios y actos de ejecución, niega la posibilidad de construir un criterio que pueda utilizarse para limitar la totalidad de los casos, por lo que confía al juez la calificación de cada caso concreto. Ver en CURY URZÚA, Enrique, *Derecho Penal*, cit. (n. 48), p. 555.

[68] Este examen por cada tipo específico se ve claramente respecto del verbo rector de cada uno. Así por ejemplo, la conducta que describe el verbo "defraudar" no es en ningún caso constitutiva de aquella expresada por el verbo "matar" o "yacer".

[69] No se debe confundir, en este sentido, el principio de ejecución "tipo por tipo", como explica la teoría de Beling, en contraposición al principio aplicado "caso por caso". Al respecto, CURY URZÚA, Enrique, *Tentativa*, cit. (n. 62), p. 34.

[70] CURY URZÚA, Enrique, *Derecho Penal*, cit. (n. 48), p. 553.

[71] Bajo la denominación de teorías mixtas, véase CURY URZÚA, Enrique, *Tentativa*, cit. (n. 62), p. 38.

[72] GARRIDO MONTT, Mario, cit. (n. 55), p. 271.

[73] CURY URZÚA, Enrique, *Tentativa*, cit. (n. 62), p. 39.

[74] CURY URZÚA, Enrique, *Derecho Penal*, cit. (n. 48), p. 556.

de forma manifiesta al hecho punible determinado[75]. En cambio, son actos equívocos, y por ende preparatorios, "los que al considerarlos en su objetividad pueden o no estar dirigidos al resultado típico"[76], de manera que este acto externo puede indistintamente encauzar tanto a un hecho inocente, como a un delito.

A su vez, se diferencia también entre actos absoluta y relativamente equívocos. Un acto es absolutamente equívoco, si aún mirado en conjunto con las demás circunstancias concurrentes no logra demostrar vinculación alguna con el delito[77] o, dicho con otras palabras, el acto es igualmente ambigüo[78].
Por el contrario, un acto es relativamente equívoco[79], si en dicha situación se "halla acompañado por condiciones materiales de una índole tal, que manifiestan, sin duda, su dirección hacia un delito determinado"[80].

Carrara abandonó esta teoría de la univocidad, recurriendo entonces a un nuevo criterio[81] de "ataque a la esfera jurídica de la víctima"[82] calificando los actos en preparatorios y de ejecución en atención a los sujetos de la acción delictiva, a saber, el sujeto activo del delito o sujetos pasivos del mismo, pudiendo ser estos últimos sujetos pasivos del atentado o de la consumación según corresponda[83]. Con esto en mente, "serían actos consumativos los que recaen sobre el sujeto pasivo de la consumación, vale decir, sobre las personas o cosas respecto de las cuales se dirige la violación definitiva del derecho (el hombre que se va a matar, la cosa que se va a robar, etc.); serían actos ejecutivos los que recaen sobre el sujeto pasivo del atentado (el domicilio invadido o la ventana forzada para cometer un hurto o robo), y serían actos preparatorios los que recaen solamente sobre el sujeto activo del delito que se prepara (rondar la casa ajena, proveerse del arma necesaria)"[84].

Por otra parte, como ya se ha mencionado, han surgido igualmente diversas teorías centradas en aspectos subjetivos del acto. Destaca en este sentido la teoría subjetiva extrema, la cual plantea que "el injusto se agota en cualquier exteriorización de una

[75] De esta forma el acto externo se torna unívoco según NOVOA, Eduardo, cit. (n. 50), p. 115.
[76] GARRIDO MONTT, Mario, cit. (n. 55), p. 272.
[77] Así por ejemplo, comprar un arma o hacer un plano de las oficinas de la entidad financiera que se pretende asaltar, tal como se plantea por GARRIDO MONTT, Mario, cit. (n. 55), p. 272.
[78] En el mismo sentido, CURY URZÚA, Enrique, *Derecho Penal*, cit. (n. 48), p. 556.
[79] Resulta un acto relativamente equívoco, por ejemplo, entrar subrepticiamente a la casa ajena con las bolsas adecuadas para recoger un botín que se encuentra en ella. Así lo plantea GARRIDO MONTT, Mario, cit. (n. 55), p. 272.
[80] CURY URZÚA, Enrique, *Derecho Penal*, cit. (n. 48), p. 556.
[81] Esta segunda formulación de Carrara, en conjunto con las de otro grupo de autores, han sido agrupados bajo la denominación de teorías materiales, en razón del carácter de los criterios que propugnan (vr.g. la puesta en peligro del bien jurídico de protección, el principio de la lesión del objeto jurídico, la idoneidad del acto), los cuales se aplicarían con prescindencia de marcos formales. Más profundamente en CURY URZÚA, Enrique, *Tentativa*, cit. (n. 62), pp. 54-56.
[82] LABATUT GLENA, Gustavo, cit. (n. 54), p. 184.
[83] Así lo describe Etcheberry bajo la denominación de la "teoría de los sujetos", la que a su juicio si bien podría funcionar de forma correcta en casos particulares de delitos –sobre todo aquellos que el mismo Carrara utiliza en sus ejemplos–, constituiría de todas formas un problema en cuanto a su aplicación para todos los delitos como regla general. Ver ETCHEBERRY ORTHUSTEGUY, Alfredo, cit. (n. 53), pp. 59-60.
[84] NOVOA, Eduardo, cit. (n. 50), p. 116.

voluntad mala que se orienta a la ejecución de una acción reprobada por el derecho o a la obtención de un resultado jurídicamente lesivo"[85]. En este sentido, todo acto es una manifestación de un propósito disvalioso y, por lo tanto, carecería de importancia la diferencia entre actos preparatorios y de ejecución por cuanto cualquiera de estos son suficientes para considerar el hecho como punible a título de tentativa[86].

Asimismo, se presenta la teoría subjetiva limitada, la cual concuerda con la concepción extrema respecto de que se inicia la tentativa en aquellos casos en que el individuo da principio a la ejecución de la conducta típica, sin embargo, tal contenido del tipo ha de configurarse de manera diversa. En efecto, se propugna al respecto una estructura típica variable y multifacética, la cual se establece para cada caso en particular en base a aquello que el individuo se haya propuesto consumar[87]. Así las cosas, "la referencia al 'plan del autor' sirve para precisar las características específicas del tipo con que, en el caso concreto, debe compararse la acción ejecutada por el autor[88]. Pero la determinación de los límites de aquélla, y el problema relativo a si ésta los ha traspuesto, sólo se decide en una segunda etapa y con arreglo a criterios objetivos"[89].

Lo dicho nos orienta claramente a una interrogante: ¿En qué etapa del *iter criminis* podemos ubicar al *phishing*?

a)El phishing como acto preparatorio

En virtud de lo analizado, una de las posibilidades que se presenta es concebir el *phishing* como un acto preparatorio. Como se ha visto, si bien en la práctica se torna difícil precisar el límite entre los actos preparatorios y los de ejecución, es de todas formas un punto fundamental en virtud de que, por regla general, los primeros no están sujetos a sanción penal[90]. De todas formas, no se debe pasar por alto que el acto preparatorio supone "ya formado el propósito de delinquir, o sea, son actos encaminados también a producir o al menos facilitar el resultado"[91]. Bajo esta lógica, cobra sentido el hecho que excepcionalmente la ley sancione actos preparatorios. Como fundamento de esto último se han planteado principalmente dos razones[92]; la primera, en atención a la índole de la conducta realizada que, a pesar de no implicar la ejecución de la acción típica, crea de

[85] CURY URZÚA, Enrique, *Derecho Penal*, cit. (n. 48), p. 558.
[86] Sobre ello en CURY URZÚA, Enrique, *Derecho Penal*, cit. (n. 48), p. 558.
[87] Abordado en profundidad por CURY URZÚA, Enrique, *Tentativa*, cit. (n. 62), pp. 63-72.
[88] Cury plantea como ejemplo del examen objetivo que se debe realizar para determinar si la conducta se ha iniciado el caso en que estando acreditado que A tenía la intención de matar a B, mediante la instalación en su domicilio de un dispositivo que activaba un arma oculta al pisarlo, lo cual no fue completado pues A es sorprendido mientras cargaba los implementos para realizar su cometido. Lo anterior no resuelve de manera inmediata si ha principiado la ejecución, sino que entrega los antecedentes necesarios para determinar la estructura del tipo "matar a otro mediante un dispositivo automático que dispara un revolver cuando lo pisa la víctima". Con detalle en CURY URZÚA, Enrique, *Tentativa*, cit. (n. 62), p. 67.
[89] CURY URZÚA, Enrique, *Derecho* Penal, cit. (n. 48), p. 560.
[90] En este sentido, LABATUT GLENA, Gustavo, cit. (n. 54), p. 180.
[91] ETCHEBERRY ORTHUSTEGUY, Alfredo, cit. (n. 53), p. 53.
[92] CURY URZÚA, Enrique, *Tentativa*, cit. (n. 62), p. 73.

todas formas una situación de peligro para el objeto de protección jurídica; la segunda, en atención a la naturaleza peculiar del bien jurídico, se ha querido proteger de una mejor manera un bien jurídico especialmente sensible a los ataques, aún cuando el acto se encuentra fuera de la descripción del tipo.

Ahora bien, en cuanto al estudio en concreto de la figura del *phishing*, ciertamente se debe aludir a los criterios que le otorgarían el carácter de preparatorio a dicho comportamiento, siendo relevantes para tales efectos los postulados de la teoría de Beling, la teoría mixta y la teoría pragmática de Carrara. No obstante, los criterios señalados no son suficientes por sí solos para calificar fundadamente el *phishing* como un acto preparatorio. En efecto, junto a ello es necesario hacer referencia a delitos concretos de nuestro ordenamiento jurídico a los que podría estar encaminada la figura en estudio, toda vez que los actos preparatorios tienden a la perpetración de un hecho delictuoso típico[93].

De esta forma, teniendo en mente el concepto de *phishing* adoptado a lo largo de este trabajo, es decir, "aquel comportamiento por el que un sujeto emplea la ingeniería social o subterfugios técnicos para engañar a otro, por medio de comunicaciones aparentemente verdaderas, logrando que este último le remita información de carácter confidencial", es posible vincular el *phishing* con diversos delitos de nuestra legislación, destacando entre ellos los delitos de hurto y robo.
Cobra especial importancia en este punto, los diversos propósitos para los que el *phisher* ha obtenido la información de carácter confidencial, pues son estos los que también servirán de guía en la búsqueda de un hecho típico al que se vería dirigida la acción del atacante.

Pues bien, una alternativa es vincular el *phishing* con ciertos delitos contra la propiedad, como la figura del hurto y el robo con fuerza en las cosas.

El primero, según el artículo 432[94] del Código Penal, puede ser definido como "la apropiación de una cosa mueble ajena, sin voluntad del dueño, con ánimo de lucrarse, y sin que concurran la fuerza en las cosas ni la violencia o intimidación en las personas"[95]. En este orden de ideas, el *phishing* podría significar una primera instancia para la posterior comisión del delito de hurto, toda vez que la información confidencial obtenida podría ser utilizada para realizar actos que afecten el patrimonio de la víctima sin su consentimiento para ello. A modo de ejemplo, si la información confidencial contenía los datos bancarios de la víctima, estos podrían ser objeto de una transferencia electrónica de dinero desde la cuenta de esta última a la cuenta del *phisher*[96]. De esta forma, finalizada

[93] Véase NOVOA, Eduardo, cit. (n. 50), p. 115.
[94] Artículo 432 Código Penal: El que sin la voluntad de su dueño y con ánimo de lucrarse se apropia cosa mueble ajena usando de violencia o intimidación en las personas o de fuerza en las cosas, comete robo; si faltan la violencia, la intimidación y la fuerza, el delito se califica de hurto.
[95] OLIVER CALDERÓN, Guillermo, *Delitos contra la propiedad* (Santiago, Legal Publishing, 2013), p. 111.
[96] Puede que la transferencia sea dirigida a cuantas pertenecientes a terceros. En estas situaciones puede que aparezca un sujeto distinto a los miembros organizados encargados de la obtención de la información confidencial, denominados "*phisher-mule"*, quienes retirarían rápidamente el dinero transferido y tras descontar su comisión, las envían por correo o empresas de envío de dinero a personas desconocidas, que

de forma exitosa la transferencia, existiría efectivamente una apropiación de una cosa mueble ajena.

En cuanto al segundo, se ha señalado que "comete el delito de robo con fuerza en las cosas quien se apropia de cosa mueble ajena, sin voluntad de su dueño, con ánimo de lucrarse y utilizando fuerza en las cosas"[97]. Se debe hacer la salvedad de que no toda fuerza forma parte de esta figura, sino que solo aquellas que el legislador ha previsto[98]. Destaca especialmente la modalidad de robo en lugar no habitado, tipificado en nuestro ordenamiento jurídico en el artículo 442[99], el cual alude al uso de llaves falsas o verdadera que ha sido sustraída[100].

Bajo esta lógica, el *phishing* podría constituir un acto preparatorio del robo con fuerza en las cosas, por cuanto las comunicaciones con la apariencia de verdaderas que sostiene el *phisher* con la víctima a partir de las cuales obtiene información de carácter confidencial podría catalogarse como una etapa preliminar de este delito, para que luego de aquella información se utilicen datos bancarios, como las claves de seguridad, para su empleo como "llaves falsas"[101] y así acceder a los sistemas bancarios de las víctimas.
De esta forma, por el uso de estas "llaves falsas" el *phisher* podría tener acceso a la cuenta bancaria del atacado pudiendo realizar transacciones electrónicas desde esta plataforma, enviando el dinero a otras cuentas manipuladas por éste.

Así, a la luz de las teorías mencionadas al comienzo del apartado, sería posible calificar el *phishing* como un acto preparatorio, pues de acuerdo con la teoría de Beling, aún no se realizaría ni la acción típica del hurto ni la correspondiente al robo con fuerza en las coas, debido a que la apropiación de la cosa mueble ajena tendría lugar posteriormente a la conducta del *phishing*. Asimismo, siguiendo la teoría mixta, la conducta sería preparatoria, ya que junto con no cumplir con la acción descrita en el tipo, de acuerdo con

---

resultan ser los *phishers.* Con más detalle en FLORES MENDOZA, Fátima, *La responsabilidad penal del denominado mulero o phisher-mule en los fraudes de banca electrónica*, en *Cuadernos de Política Criminal* 110 (2013) 2, p. 163.

[97] OLIVER CALDERÓN, Guillermo, cit. (n. 95), p. 111.

[98] MERA, Jorge, *Hurto y Robo* (Santiago, Lexis Nexis, 2004), p. 91.

[99] Artículo 442 Código Penal: El robo en lugar no habitado, se castigará con presidio menor en sus grados medio a máximo siempre que concurra alguna de las circunstancias siguientes: 1a.Escalamiento. 2a.Fractura de puertas interiores, armarios, arcas u otra clase de muebles u objetos cerrados o sellados. 3a.Haber hecho uso de llaves falsas, o verdadera que se hubiere substraído, de ganzúas u otros instrumentos semejantes para entrar en el lugar del robo o abrir los muebles cerrados.

[100] Una concepción más amplia puede ser encontrada en la legislación española. Así, el artículo 239 del Código Penal español señala: Se considerarán llaves falsas: 1. Las ganzúas u otros instrumentos análogos. 2. Las llaves legítimas perdidas por el propietario u obtenidas por un medio que constituya infracción penal. 3. Cualesquiera otras que no sean las destinadas por el propietario para abrir la cerradura violentada por el reo. A los efectos del presente 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. CÓDIGO PENAL ESPAÑOL Y LEGISLACIÓN COMPLEMENTARIA, Disponible en https://boe.es/legislacion/codigos/codigo.php?id=038_Codigo_Penal_y_legislacion_complementaria&modo=1

[101] De esta manera, se podría sostener 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. Así se plantea por OXMAN, Nicolás, cit. (n. 3), p. 240.

la concepción natural del hurto, tampoco pareciera que la conducta del *phishing* se considere incorporada en la acción del referido delito. Es decir, no es posible establecer una unión necesaria entre el comportamiento descrito en el *phishing* y el hurto. El mismo razonamiento puede ser aplicado al robo con fuerza en las cosas. Por lo demás, en atención a la teoría pragmática de Carrara, es posible calificar el *phishing* como un acto equívoco, pues, no obstante poder estar dirigida la conducta a un posterior hurto o robo, ello no es determinante, toda vez que puede bien estar dirigido a otro objetivo (la información podría no ser utilizada de aquella manera), y consecuentemente, no tendría lugar ni el hurto ni el robo en su caso.

Cabe preguntarse al respecto, de considerarse el *phishing* como un acto preparatorio, dos interrogantes principales. En primer lugar, si el comportamiento constitutivo de *phishing* merece ser sancionado y consecuentemente, en segundo lugar, qué procedimiento sería el utilizado para conseguir tal objeto.

En cuanto al primer asunto en cuestión, corresponde examinar los motivos que harían meritorios que el *phishing* fuese sancionado. En este sentido, es posible sostener que la conducta de esta figura importa cierto desvalor en atención a varios aspectos. Un primer elemento a resaltar es la presencia de un engaño por parte del *phisher* mediante el uso de la ingeniería social o subterfugios técnicos, lo cual lleva a que la víctima del ataque entregue sus datos con la convicción de que la entidad que los recibe es legítima. Asimismo, un segundo elemento a considerar es la presencia de información de carácter confidencial, que en otras circunstancias la víctima no habría entregado sin antes formular ciertos reparos en ello. Junto con ello, es preciso indicar también que la información obtenida de estas comunicaciones puede ser utilizados para diversos motivos que, por sobre todo, ponen en peligro los intereses de la víctima.

En base a lo anterior, es posible concluir que, dado los rasgos característicos del *phishing*, esta es una figura que conlleva la existencia de variados peligros para importantes bienes jurídicos como lo son la propiedad y la intimidad. Es por ello que se torna necesario que la figura del *phishing* sea considerada dentro de las excepciones en que el ordenamiento jurídico sanciona actos preparatorios.

Para otorgar respuesta a la segunda interrogante, es necesario mencionar que desde una perspectiva técnica es posible acudir a diversos procedimientos a fin de sancionar este tipo de conductas previas a la ejecución[102].

Una primera posibilidad es que la misma ley de manera expresa y directa amplíe el tipo penal y establezca la punibilidad para el sujeto que ha preparado la ejecución del mismo. Sin embargo, aún cuando este es uno de los recursos considerados de mayor sencillez y comprensión, constituye de todas formas una exagerada extensión de la punibilidad[103], "apartándose de los principios limitadores del *ius puniendi*"[104].

[102] Así se señala en base a lo postulado por el autor Maurach en BULLEMORE, Vivian, MACKINNON, John, *Curso de Derecho Penal Parte General* (Santiago, Lexis Nexis, 2007) II, p. 192.
[103] CURY URZÚA, Enrique, *Derecho Penal*, cit. (n. 48), p. 561.
[104] BULLEMORE, Vivian, MACKINNON, John, cit. (n. 102), p. 192.

Una segunda posibilidad es que la ley sancione "ciertas acciones que constituyen formas anticipadas de participación criminal"[105]. Se sitúan en este caso, la proposición y conspiración, figuras sancionadas por nuestro ordenamiento jurídico en el artículo 8[106] del Código Penal. Dentro de este marco, ha de considerarse que ambas requieren no solo de una resolución interior, sino que también de una manifestación externa. En la proposición, "el sujeto solicita a otra u otras personas que participen, conjuntamente con él, en la realización del hecho típico que está resuelto a ejecutar"[107]. Por su parte, en la conspiración, se realiza un acuerdo expreso para la ejecución del hecho típico, debiendo existir un concierto de voluntades de carácter serio por el que convienen en coejecutar el delito[108].
Las referidas conductas son impunes, salvo que la ley expresamente disponga lo contrario, como ocurre en lo establecido por nuestro Código Penal a propósito de los delitos contra la seguridad exterior e interior del Estado[109].

Una tercera posibilidad es que la ley eleve a "categoría de delito *sui géneris* ciertas conductas que preceden a la ejecución"[110]. Hay quienes se han referido a esta situación como "actos preparatorios especialmente penados"[111] respecto de los cuales, se ha anticipado la penalidad notablemente por parte del legislador para la protección de un bien jurídico. Como consecuencia de ello, tales actos adquieren el carácter de tipos legales autónomos de peligro[112]. Así las cosas, en atención a la técnica utilizada, tales figuras son constitutivas de "tipos delictivos autónomos cuya problemática, por lo tanto, es independiente de la de la tentativa. Requieren, en consecuencia, un tratamiento separado, propio de la parte especial"[113]. En este sentido, la sanción dispuesta por la ley

---

[105] BULLEMORE, Vivian, MACKINNON, John, cit. (n. 102), p. 192.
[106] Artículo 8 Código Penal: La conspiración y proposición para cometer un crimen o un simple delito, sólo son punibles en los casos en que la ley las pena especialmente. La conspiración existe cuando dos o más personas se conciertan para la ejecución del crimen o simple delito. La proposición se verifica cuando el que ha resuelto cometer un crimen o un simple delito, propone su ejecución a otra u otras personas. Exime de toda pena por la conspiración o proposición para cometer un crimen o un simple delito, el desistimiento de la ejecución de éstos antes de principiar a ponerlos por obra y de iniciarse procedimiento judicial contra el culpable, con tal que denuncie a la autoridad pública el plan y sus circunstancias.
[107] CURY URZÚA, Enrique, *Tentativa*, cit. (n. 62), p. 78.
[108] Tratado con detalle por Politoff, no debiendo ser un acuerdo de voluntades puramente aparente, como por ejemplo, si los sujetos solo discuten la posibilidad de ejecutar o si no hubieran decidido ponerlo en obra. Asimismo, el acuerdo no puede ser provisional. Señala además, que en nuestro sistema la ley solo sanciona cuando el concierto se refiere a la comisión de un crimen o simple delito. Véase en POLITOFF LIFSCHITZ, Sergio, *Los Actos preparatorios*, cit. (n. 49), pp. 75-91.
[109] En los artículos 111 y 125 respectivamente, así como también en razón de la Ley Nº 12.927 en su artículo 23 acerca de la seguridad del Estado[109] ("La proposición y la conspiración para cometer alguno de los delitos sancionados en esta ley, serán castigadas con la pena señalada al delito consumado, rebajada en uno o dos grados"). Esta medida en particular puede encontrar su fundamento en que se considere un bien jurídico digno de protección penal la seguridad, la paz o tranquilidad, individual o colectiva, constituyendo el hecho antijurídico la mera manifestación verbal de una determinación delictuosa. Véase NOVOA, Eduardo, cit. (n. 50), pp.112-113.
[110] BULLEMORE, Vivian, MACKINNON, John, cit. (n. 102), p. 192.
[111] Así se refiere a ellos en ETCHEBERRY ORTHUSTEGUY, Alfredo, cit. (n. 53), p. 53.
[112] Bajo el respecto de delito preparatorio *sui géneris*, ver en POLITOFF LIFSCHITZ, Sergio, *Los Actos preparatorios*, cit. (n. 49), pp. 48-50.
[113] CURY URZÚA, Enrique, *Tentativa*, cit. (n. 62), p. 75.

no es en atención a la naturaleza preparatoria de los actos constitutivos del hecho, sino que se considera un delito especial, diferenciable y punible de forma independiente[114]. Por tanto, en ciertos casos determinados, los actos preparatorios serán tipificados por la ley como delitos consumados[115].

Existen varios ejemplos[116] dentro de nuestro ordenamiento jurídico en que se ha optado por seguir este procedimiento. Uno de los casos más característicos es el delito descrito en el referido artículo 445, en el cual se castiga a "el que fabricare, expendiere o tuviere en su poder llaves falsas, ganzúas u otros instrumentos destinados conocidamente para efectuar el delito de robo y no diere descargo suficiente sobre su fabricación, expendición, adquisición o conservación". Como es posible apreciar, el anterior delito se considerará consumado por el solo hecho de fabricar, expender, o tener consigo los objetos allí mencionados, en un supuesto en que estén destinados para cometer un robo. En efecto, se ha señalado que uno de los elementos que demuestran que tal disposición se trata de "un acto preparatorio de la futura ejecución de un robo con fuerza en las cosas"[117], es precisamente el hecho que la disposición exija que los objetos aludidos estén "destinados conocidamente para efectuar el delito de robo",
Asimismo, se debe destacar que, a falta de estas figuras delictivas *sui géneris*, tales conductas, por aplicación de las reglas generales, resultarían impunes por constituir meros actos preparatorios de los delitos tipificados[118].

Llegados a este punto, podría considerarse el *phishing* como una figura de peligro, y bajo esto lógica, el procedimiento que mejor se ajustaría para lograr su sanción es aquel que eleva la conducta a la categoría de delito *sui géneris* con lo cual, como ya se ha mencionado, se adelantaría la protección al bien jurídico que se ve amenazado con este comportamiento.

---

[114] En esta misma línea, no se les consideraría una forma imperfecta de otro delito, al contrario, se trataría de un delito especial y punible de por sí. Al respecto ETCHEBERRY ORTHUSTEGUY, Alfredo, cit. (n. 53), p. 53.

[115] Así se considera en POLITOFF LIFSCHITZ, Sergio, *Los Actos preparatorios*, cit. (n. 49), p. 48.

[116] Existen varios ejemplos dentro de nuestro ordenamiento jurídico en que se ha optado por seguir este procedimiento, a saber, aquellos contenidos en los artículos 124 (seducción de tropas, usurpación de mando), 181[116],187[116](ambos referidos a falsificación de instrumentos tales como punzones, cuños, matrices, timbres, que pueden ser utilizados para falsificar monedas u otros objetos), 296 (amenaza de un mal constitutivo de delito), 404[116](provocación a duelo), 445 y 481 (aprehendido con artefactos, implementos o preparativos conocidamente dispuestos para incendiar o causar alguno de los estragos expresados) del Código Penal. Cury menciona diversos ejemplos de esta índole en CURY URZÚA, Enrique, *Derecho* Penal, cit. (n. 48), p. 561. Así también LABATUT GLENA, Gustavo, cit. (n. 54), p. 181.

[117] Tomando para ello como base lo discutido en la sesión nº93 de la Comisión Redactora del Código Penal, por cuanto la finalidad de la modificación del artículo era que en todos los casos se exigía un conocimiento cierto del destino que tendría la llave o instrumento, tratándose en consecuencia de una figura de peligro concreto. Se debe tener en cuenta, en todo caso, que en su carácter de delito preparatorio se le reconoce una subsidiariedad tácita en relación con la efectiva comisión del delito de robo en particular, pues de ser así el caso, no es posible castigar el delito consumado de robo sancionado por el art. 440 nº2 del Código Penal en conjunto con el delito tipificado en el ya mencionado art. 445, debido a que en este caso rige ampliamente el principio *non bis in ídem.* Siendo para ambos delitos el mismo sujeto activo, se produciría en tanto un concurso aparente de leyes penales, debido a que la pena establecida para esta figura "al ser menor que la del robo, se ve absorbida por éste". Véase OLIVER CALDERÓN, Guillermo, cit. (n. 95), p. 269.

[118] Véase ETCHEBERRY ORTHUSTEGUY, Alfredo, cit. (n. 53), p. 55.

b) El phishing como tentativa de delito en sentido amplio

En directa relación con el apartado anterior, existe otra etapa del *iter criminis* en la que podría ser subsumido el *phishing*, ello debido a que "más allá de los actos preparatorios se encuentran los actos de ejecución, que constituyen el conato o tentativa en sentido amplio"[119]. Esto tiene una especial consecuencia debido a que, por regla general, estos últimos actos son sancionados por el ordenamiento jurídico[120].

Cabe destacar que se han propuesto diversas teorías para fundamentar la punibilidad de estos actos que preceden a la consumación del delito.

Primero, se plantea la teoría objetiva o clásica, según la cual "los comportamientos típicos merecen castigo exclusivamente cuando lesionan o ponen en peligro un bien jurídico digno de protección"[121]. En este sentido, el peligro aludido debe crearse efectivamente y ser de carácter serio, respecto de la lesión que puede materializarse[122].
Por lo tanto, de producirse lesión, el hecho necesariamente debe ser sancionado; si, en cambio, el bien jurídico solo fue puesto en peligro, la conducta también será penada pero bajo una menor sanción; por último, si no se provoca lesión o peligro, no procede castigo alguno[123].

Segundo, se alza también una teoría subjetiva, de acuerdo con la cual aquello meritorio de sanción es "la voluntad rebelde expresada en la ejecución total o parcial del acto"[124]. En consecuencia, lo castigado es la conducta en sí misma, puesto que existe una voluntad en contra del orden normativo[125]. Así pues, se ha dicho que "lo esencial del hecho punible consiste en la violación de un deber de obediencia al Estado y en la rebelión de la voluntad del delincuente contra la voluntad colectiva expresada en la ley"[126].

Tercero, es posible encontrar también una teoría mixta o ecléctica, la cual considera como punible, al igual que la concepción subjetiva, aquella voluntad rebelde del sujeto, a lo que agrega como elemento objetivo a considerar que la conducta seguida por el individuo origine en el ordenamiento jurídico un estado de conmoción[127]. De esta manera, si bien aquello sancionado es la voluntad contraria a derecho, "la exteriorización

[119] ETCHEBERRY ORTHUSTEGUY, Alfredo, cit. (n. 53), p. 57.
[120] El intento se considera, en principio, también merecedor de pena. Se excluirían en tanto, las faltas y delitos culposos. Véase en POLITOFF LIFSCHITZ, Sergio, *Los Actos preparatorios*, cit. (n. 49), p. 20.
[121] GARRIDO MONTT, Mario, cit. (n. 55), p. 263.
[122] CURY URZÚA, Enrique, *Derecho* Penal, cit. (n. 48), p. 574.
[123] Así se explica en GARRIDO MONTT, Mario, cit. (n. 55), p. 263.
[124] CURY URZÚA, Enrique, *Derecho Penal*, cit. (n. 48), p. 574.
[125] A ello se refiere Garrido, señalando que esta es la doctrina que adoptó el positivismo italiano, valorando especialmente el *animus necandi* del sujeto. Ver en profundidad GARRIDO MONTT, Mario, cit. (n. 55), p. 264.
[126] NOVOA, Eduardo, cit. (n. 50), p. 108.
[127] GARRIDO MONTT, Mario, cit. (n. 55), p. 265.

de esa voluntad debiera ser para perturbar la confianza de la colectividad en la vigencia del ordenamiento jurídico y el sentimiento de seguridad jurídica"[128].

De las anteriores concepciones expuestas, es posible distinguir dos perspectivas en cuanto a la mayor o menor penalidad de los actos que preceden a la consumación del delito. Es así que, como corolario de la teoría subjetiva, es posible establecer una igualación del castigo del delito consumado y los actos que le preceden[129]. Por otro lado, respecto de la teoría objetiva, se diferencia entre una categoría y otra, por cuanto respecto de los actos anteriores al delito consumado es posible exigir "un tratamiento penal menos severo"[130]. Esta distinción se establece en virtud de que, en el caso del delito consumado, el interés protegido por la norma se ha visto dañado, en cambio, para el caso del delito intentado, este interés solo ha corrido peligro[131].

Asimismo, se ha planteado que "por no haberse completado las exigencias de la figura legal (por faltar el resultado), el contenido de injusto es menor que en el delito consumado, lo que justifica que la pena aplicable sea menor"[132].

Bajo este respecto, la doctrina nacional ha adoptado de forma unánime esta última perspectiva que propugna un injusto menor, considerando que el ordenamiento jurídico se perturba de una manera más profunda con la concurrencia de un delito consumado[133].

Ahora bien, se ha aludido al término de conato o tentativa en sentido amplio, tendencia que se ha tornado cada vez más frecuente en las regulaciones más modernas[134]. Sin embargo, se debe mencionar que nuestro ordenamiento jurídico ha seguido un criterio más clásico –frecuentemente utilizado en la época de su dictación– por lo que distingue dentro del concepto amplio de tentativa, entre simple tentativa y delito frustrado[135], los que se encuentran sancionados en el artículo 7[136] del Código penal.

En palabras simples, habrá tentativa de crimen o simple delito en aquellos casos en que "el sujeto, con el propósito de consumar, inicia la ejecución de la acción típica, pero no

[128] POLITOFF LIFSCHITZ, Sergio, *Los Actos preparatorios*, cit. (n. 49), p. 119.
[129] Bajo la referencia de "parificación del castigo", ver CURY URZÚA, Enrique, *Derecho* Penal, cit. (n. 48), p. 575.
[130] *Ibidem*, p. 575.
[131] Véase para las consecuencias de la concepción GARRIDO MONTT, Mario, cit. (n. 55), p. 264.
[132] POLITOFF LIFSCHITZ, Sergio, *Los Actos preparatorios*, cit. (n. 49), p. 23.
[133] *Ibidem*, p. 24.
[134] La dualidad de tentativa y delito frustrado tiende a desaparecer en los Códigos modernos. Así se relata en CURY URZÚA, Enrique, *Derecho* Penal, cit. (n. 48), p. 575.
[135] Con más detalle en POLITOFF LIFSCHITZ, Sergio, *Los Actos preparatorios*, cit. (n. 49), p. 24.
[136] Artículo 7 Código Penal: Son punibles, no sólo el crimen o simple delito consumado, sino el frustrado y la tentativa. Hay crimen o simple delito frustrado cuando el delincuente pone de su parte todo lo necesario para que el crimen o simple delito se consume y esto no se verifica por causas independientes de su voluntad. Hay tentativa cuando el culpable da principio a la ejecución del crimen o simple delito por hechos directos, pero faltan uno o más para su complemento.

consigue[137] concluirla"[138]. Por su parte, habrá crimen o delito frustrado en situaciones en que "el sujeto activo realiza dolosamente la totalidad de la actividad delictiva que personalmente le correspondía ejecutar pero el curso causal que pone en movimiento no se concreta en el resultado típico perseguido por razones ajenas a su voluntad"[139].

No obstante la anterior distinción, este apartado tendrá como objeto central de análisis la figura de tentativa desde una perspectiva amplia, por lo que en su generalidad, este concepto será comprensivo de las dos figuras que nuestro ordenamiento jurídico incluye.

Ahora bien, en cuanto a la estructura de la figura de tentativa, es posible distinguir dos fases:

Por un lado, se presenta una faz subjetiva, siendo su elemento central el dolo[140], el cual es el mismo tanto para la tentativa como para el delito consumado[141]. Es decir, "no existe un dolo de tentativa"[142] y, por lo mismo, no existiría dolo si únicamente se tuviese voluntad para iniciar el hecho típico, mas no para consumarlo[143]. Se requiere, pues, "que el sujeto se represente la ejecución de todo el hecho integrante del tipo legal y que quiera, asimismo, su realización completa"[144].

Igualmente, deben concurrir "los demás elementos subjetivos del tipo distintos del dolo (elementos subjetivos del injusto), cuando son exigidos por la correspondiente figura de consumación"[145].

Por otro lado, se encuentra una faz objetiva, para la cual se torna necesario establecer un límite a fin de precisar desde qué momento será punible la conducta que se dirigirá a la consumación del hecho típico. En este punto cobran nuevamente relevancia las teorías objetivas y subjetivas ya expuestas en líneas anteriores[146].

Lo dicho ha sido planteado por otros autores como elementos integrantes de la tentativa, con la cual se agrega a los ya mencionados principio de ejecución del delito e intención

[137] Al faltar uno o más actos para terminar la ejecución de la acción típica, lo que ocurre es que no se logra terminar toda la actividad material personal que esta supone. Así se entiende en GARRIDO MONTT, Mario, cit. (n. 55), p. 268.
[138] CURY URZÚA, Enrique, *Derecho* Penal, cit. (n. 48), p. 552.
[139] GARRIDO MONTT, Mario, cit. (n. 55), p. 268.
[140] Tanto la doctrina nacional como extranjera ha manifestado diversas opiniones respecto de la aceptación del dolo eventual como elemento subjetivo de la tentativa. La postura afirmativa a esta problemática es la que ha prevalecido como tesis dominante. Así se plantea en CURY URZÚA, Enrique, *Tentativa*, cit. (n. 62), p. 95. Sin embargo, este mismo autor ha cambiado su parecer, considerando incompatible los objetivos que se tienen durante la tentativa con el dolo eventual, tal como lo plantea en CURY URZÚA, Enrique, *Derecho* Penal, cit. (n. 48), p. 562.
[141] GARRIDO MONTT, Mario, cit. (n. 55), p. 269.
[142] CURY URZÚA, Enrique, *Derecho* Penal, cit. (n. 48), p. 562.
[143] A favor de esta postura, GARRIDO MONTT, Mario, cit. (n. 55), p. 270.
[144] CURY URZÚA, Enrique, *Tentativa*, cit. (n. 62), p. 94.
[145] CURY URZÚA, Enrique, *Derecho* Penal, cit. (n. 48), p. 563.
[146] Esto fue desarrollado en la página 16 de este trabajo.

de alcanzar el resultado delictivo (dolo), un tercer elemento referido a la interrupción de la actividad criminal, por causas ajenas a la voluntad del agente[147].

Cabe hacer referencia en este punto a ciertas características principales que presenta la tentativa. Así pues, en relación al esquema del delito, se trataría de una figura de carácter accesorio, la cual está vinculada con una figura delictiva autónoma. Bajo esta lógica, si se considera la primera de forma aislada esta carecería de significación, sin embargo, esto cambia al relacionarla con el delito principal correspondiente, por cuanto adquiere el carácter de causa de extensión del tipo a situaciones que normalmente serían atípicas[148]. Se entiende entonces que "el precepto que extiende la punibilidad a los hechos tentados carece de autonomía y funciona solamente en relación con otro precepto que es el autónomo o principal, encargado de dar la descripción del tipo como hecho consumado"[149]. Por causa de lo anterior, es que se ha negado la posibilidad de referirse a la tentativa en abstracto, prescindiendo de un vínculo con un delito determinado[150].

Otra característica que se debe mencionar, respecto del resultado, es que desde una concepción objetiva la tentativa se ha considerado por algunos autores como un delito imperfecto[151], por cuanto con su realización no es posible alcanzar la consumación del delito[152].

De lo anteriormente expuesto, ya es posible inferir que el examen del *phishing* en cuanto tentativa en sentido amplio está incompleto si no se analiza con qué delito autónomo o principal podría estar vinculado.

Por tanto, teniendo en consideración el concepto de *phishing* que se ha adoptado a lo largo de este trabajo, una primera posibilidad que se debe analizar es establecer un vínculo con el delito de estafa[153], figura[154] que puede ser definida como aquella "conducta engañosa, con ánimo de lucro injusto, propio o ajeno que, determinando un error en una o varias personas, las induce a realizar un acto de disposición, consecuencia del cual es un perjuicio en su patrimonio o en el de un tercero"[155].

---

[147] Lo plantea se esta forma, pudiendo afirmar la existencia de elementos positivos y negativos, en LABATUT GLENA, Gustavo, cit. (n. 54), p. 183.
[148] LABATUT GLENA, Gustavo Labatut, cit. (n. 54), p. 182.
[149] NOVOA, Eduardo, cit. (n. 50), p. 109.
[150] LABATUT GLENA, Gustavo, cit. (n. 54), p. 182.
[151] Otros autores, en cambio, se han referido a ella en cuanto tipo de injusto dependiente, como un "tipo incompleto", pues faltan uno o más hechos directos para su complemento. Véase POLITOFF LIFSCHITZ, Sergio, *Los Actos preparatorios,* cit. (n. 49), p. 148.
[152] LABATUT GLENA, Gustavo, cit. (n. 54), p. 182.
[153] Así se afirma en FERNÁNDEZ TERUELO, Javier, *Respuesta penal frente a fraudes cometidos en internet: estafa, estafa informática y los nudos de la red,* en *Revista de Derecho Penal y Criminología* 19 (2007) 2, p. 233.
[154] El profesor Silva destaca una serie de problemas a nivel nacional y de derecho comparado que surgen al estudiar la figura de la estafa, debido a la diversidad de formas en que puede ser cometida, "ya que ello depende de la inteligencia e ingenio del autor y de la variedad de medios que se pueden crear". Ver SILVA SILVA, Hernán *Las Estafas* (Santiago, Editorial Jurídica de Chile, 2005), p. 27.
[155] ANTON ONECA, José, *Las estafas y otros engaños*, en *Nueva Enciclopedia Jurídica,* tomo IX (Barcelona, Editorial Francisco Seix, Barcelona, 1957), p. 57.

En este sentido, habitualmente se han señalado como elementos constitutivos de la estafa[156] el engaño, el error, el perjuicio, el ánimo de lucro y la relación de causalidad, ello sin perjuicio de que algunos autores pongan más énfasis en unos que en otros[157]. En cuanto al engaño, concebido por algunos como el elemento más característico de este delito, es concebido como la "falta de verdad en lo que se dice, hace, cree, piensa o discurre. Es pues, la acción o efecto de engañarse o sea de dar a la mentira apariencia de verdad; de inducir a sí mismo o a otro a creer y tener por cierto lo que no lo es, valiéndose de palabras, razonamientos u obras aparentes y fingidas"[158]. Cabe destacar que a la hora de definir el engaño típico tradicionalmente se ha recurrido a la llamada teoría *mise en scène* o puesta en escena, esto es, "el crear una apariencia externa que dé sustento a las manifestaciones del autor del delito"[159], cuyo objetivo es otorgar credibilidad a la mentira por medio de la disposición de ardides[160].

Asimismo, se debe tener en cuenta que no cualquier engaño es suficiente para configurar el delito de estafa, por cuanto la doctrina ha adicionado ciertos requisitos para tales efectos, a saber, que sea adecuado, serio y capaz o suficiente para influir en la voluntad de la víctima y producir el error[161]. Este último elemento mencionado es también considerado como fundamental, surgiendo como consecuencia del ya referido engaño. Así las cosas, el error ha de ser entendido como la "falsa noción que se tiene de algo; representación equivocada de un objeto cierto"[162].

Por su parte, también se encuentra el perjuicio, el cual consiste en todo detrimento o menoscabo del patrimonio, valorable económicamente[163]. Cabe resaltar al respecto que es un elemento que completa la figura de la estafa, cuya concurrencia determina que este delito se consume.

En tanto, como consecuencia del error, el engañado ha de realizar una disposición patrimonial, por la cual voluntariamente causa una disminución en su patrimonio o en el de un tercero[164].

Respecto del elemento "ánimo de lucro", su admisión ha sido polémica en nuestro ordenamiento jurídico, toda vez que la mayoría de los autores lo rechazan en base a que

---

[156] Se debe mencionar que el Código Penal chileno no define conceptos esenciales para esta figura como es el de engaño o perjuicio. Es por ello por lo que han sido la doctrina y la jurisprudencia las encargadas de proponer un concepto y esquema de los elementos típicos de la misma. Así se ha explicado en BALMACEDA HOYOS, Gustavo, *El delito de Estafa* (Santiago, Legal Publishing, 2012), p. 4.
[157] Al respecto véase con detalle SILVA SILVA, Hernán, cit. (n. 154), pp. 35-57.
[158] GOLDSTEIN, Raúl, *Diccionario de derecho penal y criminología* (Buenos Aires, Editorial Astrea, 1983), p. 291.
[159] Sentencia Rol 203-2007 6 febrero de 2008 Iltma. Corte de Apelaciones de Arica.
[160] BALMACEDA HOYOS, Gustavo, *El delito de estafa en la jurisprudencia chilena*, en *Revista de Derecho de la Universidad Austral de Chile*, 24 (2011) 1, p. 69.
[161] SILVA SILVA, Hernán, cit. (n. 154), p. 38.
[162] GOLDSTEIN, Raúl, cit. (n. 158), p. 297.
[163] BALMACEDA HOYOS, Gustavo, *El delito*, cit. (n. 156), p. 49.
[164] Se señala la postura de diversos autores en SILVA SILVA, Hernán, cit. (n. 154), pp. 50-52.

no existiría en la legislación chilena la exigencia de algún ánimo especial[165]. Sin embargo, quienes se muestran con una posición favorable se basan, entre otras cosas, en que la estafa no consiste solamente en un delito de daño contra el patrimonio, sino que también de enriquecimiento[166].

Finalmente, se encuentra una relación de causalidad entre todos los elementos ya señalados, especialmente entre el engaño y el error, así como también entre el error y la disposición patrimonial perjudicial.

Al respecto, es posible destacar también ciertas características de esta figura; primero, que este delito solo admite ser cometido por conductas dolosas, es decir, con "la voluntad de ejecutar la conducta con la intención de provocar un error en el sujeto pasivo mediante el engaño"[167]; segundo, que es posible clasificar esta figura como un delito de resultado o material, debido a que se requiere que se produzca efectivamente un perjuicio en el patrimonio del sujeto pasivo[168].

Teniendo en cuenta todo lo anteriormente dicho, sería posible subsumir el *phishing* bajo esta figura, toda vez que comparten ciertos elementos característicos. En efecto, se ha descrito el *phishing* como un comportamiento por el que un sujeto emplea la ingeniería social o subterfugios técnicos para engañar a otro, cumpliendo de esta forma con el requisito considerado esencial de la estafa. En este sentido, las llamadas "actualizaciones de seguridad" o el uso de imágenes corporativas imitadas dan cuenta de la existencia de las maniobras fraudulentas que constituyen el engaño. Asimismo, es posible distinguir el error que se provoca en la víctima, en tanto se ha formado la convicción de que el mensaje enviado por el *phisher* tiene el carácter de verdadero. Junto con ello, se podría considerar como parte de la disposición patrimonial exigido por esta figura el hecho de que la víctima del ataque entregue al emisor del mensaje información confidencial. Como es posible observar, siguiendo la definición de *phishing* adoptada en este estudio[169], surgen dudas respecto a si ciertos elementos de la estafa tienen lugar en la primera figura. Ciertamente, podría considerarse forzoso el considerar que existe disposición patrimonial por el solo hecho de entregar información confidencial, ya sea referida a nombres de usuario, contraseñas, números de tarjetas de crédito, o claves de cuentas bancarias.

De igual modo, resulta también dificultoso señalar la existencia de un perjuicio patrimonial efectivo como consecuencia de la conducta desarrollada en el *phishing*. Por lo tanto, faltando uno o más elementos de la acción típica, si bien no es posible considerarlo como constitutivo de estafa consumada, es perfectamente admisible y notorio que se configure una tentativa de estafa.

---

[165] En este sentido, POLITOFF, Sergio; MATUS, Jean Pierre y RAMÍREZ, María Cecilia, *Lecciones de Derecho Penal chileno, Parte Especial* (Santiago, Editorial jurídica de Chile, 2005), p. 419. Así también, ETCHEBERRY ORTHUSTEGUY, Alfredo, *Derecho Penal, Parte Especial* (Santiago, Editorial Jurídica de Chile, 1998), p. 402.

[166] BALMACEDA HOYOS, Gustavo, *El delito de estafa en la jurisprudencia*, cit. (n. 160), p. 67.

[167] SILVA SILVA, Hernán, cit. (n. 154), p. 66.

[168] BALMACEDA HOYOS, Gustavo, *El delito*, cit. (n. 156), p. 50.

[169] Cabe recordar que hay autores que agregan otro elemento constitutivo del *phishing*, referido al acto de tomar la información recabada y hacer uso de ella. Véase MIRÓ, Fernando, cit. (n. 4), p. 73.

Así las cosas, la doctrina ha entendido que "se presentará la tentativa cuando el culpable da principio a la ejecución de la estafa por hechos directos, por medios idóneos que constituyen engaño, pero ésta no se consuma por faltar uno o más elementos para su complemento"[170].

Asimismo, en cuanto al elemento del perjuicio, se ha dicho que si solo tiene lugar un peligro de perjuicio, mas no un perjuicio efectivo y actual, "se estará en terreno de la tentativa, pero no de la tipicidad completa de la acción punible"[171].

Otra alternativa es vincular el *phishing* con el delito de estafa informática, con el cual se hace referencia "exclusivamente a las defraudaciones 'patrimoniales' ocasionadas por medios informáticos"[172]. Esta figura ha sido recogida por diversas legislaciones del Derecho comparado europeo, destacando el modelo alemán, el italiano y el español. De esta manera, por regla general, el legislador comparado ha considerado como conducta típica de este delito a la "manipulación informática"[173].

Siguiendo el modelo español[174], el anterior término puede ser entendido como aquel en que "la máquina informática o mecánica, actúe a impulsos de una actuación legítima que bien puede consistir en la alteración de los elementos físicos, de aquellos que permiten su programación, o por la introducción de datos falsos"[175]. Sin embargo, algunos han optado por un concepto más amplio del mismo, por cuanto se ha considerado como "la realización de todo tipo de operaciones que supusiesen un incorrecto uso o provocasen un incorrecto funcionamiento de un sistema de procesamiento de datos"[176]. Asimismo, este modelo alude a la ocurrencia de un resultado típico, debiendo existir una transferencia no consentida de un activo patrimonial.

No obstante, se deben mencionar ciertas dificultades para la subsunción del *phishing* tradicional en esta figura. En primer lugar, el comportamiento al que alude el *phishing* hace referencia a la concurrencia de personas, sea el *phisher*, sea la víctima del ataque. Bajo esta lógica, "efectivamente ha existido un sujeto (persona) engañado y no

---

[170] SILVA SILVA, Hernán, cit. (n. 154), p. 123.
[171] CREUS, Carlos, *Derecho penal parte especial* (Buenos Aires, Editorial Astrea, 1983), p. 476.
[172] Se plantea una relación de género-especie entre el "fraude informático" y la "estafa informática" respectivamente. Véase BALMACEDA HOYOS, Gustavo, *El delito de estafa informática en el derecho europeo continental*, en *Revista de Derecho y Ciencias Penales* 17 (2011), p. 112.
[173] El concepto mismo de "manipulación electrónica" no ha quedado exenta de controversia. Así lo explica BALMACEDA HOYOS, Gustavo, *El delito de estafa informática*, cit. (n. 172), p. 146.
[174] Tipificado por el legislador español en el artículo 248.2 de su Código Penal: "También se consideran reos de estafa: a)Los que, con ánimo de lucro valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro". CÓDIGO PENAL ESPAÑOL Y LEGISLACIÓN COMPLEMENTARIA, disponible en https://boe.es/legislacion/codigos/codigo.php?id=038_Codigo_Penal_y_legislacion_complementaria&modo=1
[175] FERNÁNDEZ TERUELO, Javier, *Derecho* Penal, cit. (n. 25), p. 50.
[176] Siguiendo el planteamiento de Galán Muñoz, BALMACEDA HOYOS, Gustavo, *El delito de estafa informática*, cit. (n. 172), p. 138.

simplemente una máquina receptora de la maniobra fraudulenta o ardid electrónico"[177]. En segundo lugar, no existe en el *phishing* una alteración de elementos físicos ni la introducción de datos falsos, sino que la información confidencial recabada por el *phisher* proviene del propio titular de la información quien es víctima del ataque y consecuentemente, entrega de forma voluntaria –aunque viciada– aquellos datos.

Sin perjuicio de lo anterior, se debe recordar que existen formas de ejecución del *phishing* más avanzadas, como aquellas que se cometen por el uso de un *malware*, sean *keyloggers*, *screenloggers*, o *spywares*, en cuyo caso sí resultaría más lógico identificar el *phishing* con la estafa informática, toda vez que en estas situaciones "se trata de archivos que, una vez introducidos en el ordenador sin que la víctima sea consciente de ello, envían a través de la Red las claves de acceso a diferentes servicios informáticos y entre ellos las de banca *on-line*, con las cuales el defraudador puede realizar una disposición fraudulenta a su favor o a favor de un tercero"[178]. De esta forma, podría considerarse estos *malware* como una manipulación electrónica a partir de la cual el atacante obtiene información confidencial que podría tener como consecuencia una posterior transferencia de activos patrimoniales.

Por otro lado, se debe señalar que en nuestro ordenamiento jurídico no existe tipificación expresa[179] de la estafa informática[180], lo cual torna más difícil aún la imputación del *phishing* bajo este título. A falta de ello, se ha intentado asimilar la figura con alguno de los delitos descritos por la Ley Nº 19.223, que "tipifica figuras penales relativas a la informática". Desde ya, se debe mencionar que dicha normativa ha sido ampliamente criticada debido a que se le considera incompleta, confusa y desactualizada[181].

En cuanto al contenido de la referida ley, se debe mencionar que es posible distinguir dos figuras principales. Por un lado, el sabotaje informático –que se encontraría en el artículo 1 y 3–, que comprende las posibles alteraciones o manipulaciones, tanto de los datos como de los programas de un sistema computacional. Por otro lado, el espionaje informático –reconocido en los artículos 2 y 4–, que incluye la obtención dolosa, ilícita y sin autorización de datos y de programas computacionales[182].

---

[177] ROSENBLUT GORODINSKY, Verónica, *Punibilidad y tratamiento jurisprudencial de las conductas de phishing y fraude informático*, en *Revista del Ministerio Público* 35 (2008), p. 258.
[178] FERNÁNDEZ TERUELO, Javier, *Respuesta penal*, cit. (n. 153), p. 233.
[179] En efecto, pese a que en el año 2002 ingresó a la Cámara de diputados un proyecto de ley para sancionar el "fraude informático" (con una tipificación muy similar a la española), este proyecto fue archivado por considerarse que ya se ha legislado sobre esta materia. Véase Boletín 3009-07 del SENADO DE LA REPÚBLICA DE CHILE, disponible en http://www.senado.cl/appsenado/templates/tramitacion/index.php#
[180] Así lo afirma OXMAN, Nicolás, cit. (n. 3), p. 237. Con esta misma idea BALMACEDA HOYOS, Gustavo, *El delito de estafa informática*, cit. (n. 172), p. 111.
[181] Por lo demás, se ha cuestionado el método utilizado al tipificar estos delitos, ya que se prefirió la creación de una ley especial por sobre la incorporación de esta figuras en el código. Con más detalle en SILVA SILVA, Hernán, cit. (n. 154), pp. 201-217.
[182] MOSCOSO ESCOBAR, Romina, *La ley 19.223 en general y el delito de hacking en particular*, en *Revista Chilena de Derecho y Tecnología* 3 (2014) 1, p. 14.

Así las cosas, algunos autores[183] proponen la subsunción del *phishing* bajo la figura tipificada en el artículo 1[184] de la ley, "en la medida que para lograr la captura fraudulenta de datos se habría modificado o alterado un sistema de tratamiento de información"[185]. Bajo esta lógica, podría tratarse de aquellas formas de ejecución en las que se utilizan programas maliciosos, como por ejemplo un *spyware*. No obstante, según esta perspectiva, no sería posible perseguir ni castigar mediante un delito informático aquellas situaciones en que la información confidencial es obtenida en su forma más clásica, la cual es por el envío masivo de correos electrónicos.

Siguiendo con el análisis de las figuras autónomas con las que se puede vincular el *phishing*, otra posibilidad que se debe tener en cuenta es recurrir a las figuras de hurto y robo, las que ya han sido definidas anteriormente[186].
En cuanto al delito de hurto, son varios los inconvenientes que surgen a primera vista al intentar subsumir el *phishing* bajo esta figura, ello en virtud de que los elementos de ambas figuras son un tanto disímiles. En cuanto al objeto material del delito de hurto, este debe tratarse de una cosa corporal, mueble, ajena, susceptible de apropiación y apreciación pecuniaria[187].

Sin embargo, se ha señalado que resulta complejo afirmar que en el *phishing* se está en presencia de una cosa corporal mueble en sentido estricto. En efecto, se trata mas bien de la transferencia de datos o información, por lo que se ha dicho que "en estas otras conductas el objeto material no es una cosa mueble, sino paradójicamente un objeto inmaterial, datos relativos a la identidad de una persona"[188].
Por otro lado, el hurto exige que la apropiación se realice sin la voluntad del dueño, empero, en la figura del *phishing*, más que carecer de ella, se asimila de mejor forma con una voluntad viciada. Ciertamente, en esta última figura es la propia víctima quien entrega los datos de forma voluntaria, con la convicción de que se trata de una comunicación verdadera[189].

En cuanto al delito de robo, en tanto robo con fuerza en las cosas, se ha señalado que, podría ser subsumida la figura del *phishing* en este delito, si se considera que las claves de entrada a los sistemas bancarios o incluso, ciertas claves de seguridad creadas para la transferencia electrónica (obtenidas por medio de las comunicaciones aparentemente

[183] Otros autores han intentado vincular la figura del *phishing* con el artículo 2 de la ley en análisis, sin embargo, en su análisis es posible distinguir una serie de obstáculos para lograrlo, por lo que finalmente se concluye que no resulta posible recurrir a este delito. Con más detalle en OXMAN, Nicolás, cit. (n. 3), pp. 232-237.
[184] Artículo 1 Ley 19.223: El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo. BIBLIOTECA DEL CONGRESO NACIONAL disponible en https://www.leychile.cl/Navegar?idNorma=30590&buscar=19223
[185] Así se plantea en ROSENBLUT GORODINSKY, Verónica, cit. (n. 177), p. 256.
[186] Esto fue tratado en la página 19 de este trabajo.
[187] OLIVER CALDERÓN, Guillermo, cit. (n. 95), pp. 94-110.
[188] Así se indica en FLORES, Fátima, *Respuesta*, cit. (n. 37), p. 313.
[189] Referencias a los problemas de esta postura en OXMAN, Nicolás, cit. (n. 3), pp. 240-241.

verdaderas constitutivas de *phishing*), pueden ser asimiladas a las referidas "llaves falsas".[190]

No obstante lo anterior, junto con darse por reproducidas las dificultades señaladas respecto del delito de hurto, se agrega el problema de que en el ámbito en el que se sitúa el *phishing*, no se trata de un lugar físico propiamente tal, toda vez que el comportamiento tiene lugar a través de plataformas electrónicas. Esto último tiene especial importancia, debido a que la reglamentación de este delito se realiza precisamente en base a dos criterios, a saber, el medio empleado y el lugar[191] donde se lleva a cabo la apropiación de las cosas[192].

Respecto de los dos últimos delitos mencionados, y en atención a la serie de inconvenientes que conllevan, podría resultar forzoso intentar el castigo del *phishing* bajo estas figuras, aún a título de tentativa.

Dicho esto, estamos en condiciones de realizar un examen acabado de la figura del *phishing* a título de tentativa en sentido amplio, teniendo para ello en cuenta los elementos que lo componen. Así las cosas, es posible identificar el elemento subjetivo, toda vez que la conducta del *phisher* estará orientada de forma dolosa a la comisión de alguno de los delitos que se han mencionado precedentemente – existiría por tanto, un dolo de estafa o de estafa informática–. Por otra parte, podemos distinguir también la presencia del elemento objetivo de la tentativa, utilizado para ello los criterios entregados por la doctrina.

De esta forma, siguiendo la teoría subjetiva limitada, se podría considerar el *phishing* como parte de la estructura típica del delito de estafa toda vez que el *phisher* ha actuado con el propósito de defraudar a la víctima. Por tanto se iniciaría la tentativa de estafa si se ha dado principio a la ejecución de la conducta típica, que se ha de precisar de acuerdo a las características propias entregadas por el *phishing*. En efecto, esto tendría lugar por la presencia principalmente del engaño y del error, en la medida de que haya empleado algún ingeniaría social o subterfugio técnico para lograr una convicción en la víctima de que la comunicación sostenida con el atacante es verdadera.
Lo mismo es posible observar desde la perspectiva del delito de estafa informática, si el *phisher* se propone realizar una transferencia no consentida de un activo patrimonial. En este sentido, el *phishing* sería parte de las características específicas de la estafa informática, y por tanto, existiría un principio de ejecución al tener lugar una "manipulación electrónica" por medio del uso de un *malware.*

[190] De esta manera, se podría sostener 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. Así se plantea por OXMAN, Nicolás, cit. (n. 3), p. 240.
[191] Se hace referencia a los términos de "lugar" y "sitio", siendo el primero una extensión de terreno delimitada y rodeada por resguardos o defensas que impiden una entrada no autorizada, pudiendo ser catalogado como lugar habitado, destinado a la habitación o lugar no habitado. El segundo en tanto, corresponde a una extensión de terreno que no está delimitada o que carece de resguardos que impidan un ingreso no autorizado. Así lo ha entendido OLIVER CALDERÓN, Guillermo, cit. (n. 95), p. 217.
[192] MERA, Jorge, cit. (n. 98), p. 90.

En cuanto a las denominadas teorías objetivas, en atención a la concepción mixta, podría considerarse el *phishing* como un acto ejecutivo, pues se efectúa una parte de la descripción típica. En el caso de la estafa, el *phishing* pareciera tener una necesaria conexión con la acción típica de la primera, por cuanto si se sigue una concepción natural de aquella actividad se podrá observar que el engaño es un elemento inherente de ambas conductas, y específicamente en el *phishing*, el engaño se podría ver conformado por el empleo por parte del *phisher* de la ingeniería social o los subterfugios técnicos.

Asimismo, podría considerarse el *phishing* como parte del contenido del hecho típico del delito de estafa informática, si se establece una unión necesaria entre ambas conductas. De esta forma, esta conexión podría tener lugar si se incorpora en la noción de "manipulación electrónica", en tanto conducta típica, el uso de un *malware* (v.gr. un *spyware*). Por tanto, existiría un acto ejecutivo por el empleo de estos programas, realizando una parte de la descripción típica.

En tanto, de acuerdo con la teoría pragmática de Carrara, según la cual se distingue entre actos unívocos y equívocos, el *phishing* podría ser considerado siempre como un acto de ejecución, y castigarse a título de tentativa[193], en caso de ser un acto externo unívocamente dirigido a la realización de un delito[194]. De otro modo, en caso de estimarse que el *phishing* se trata de un acto equívoco –y, por ende, preparatorio–, este podría constituir de todas formas un principio de ejecución de acuerdo a las circunstancias del caso. De esta forma, si los actos preparatorios contingentes o condicionales "se hallan acompañados por condiciones materiales de una índole tal, que manifiesta sin duda su dirección hacia un delito determinado, pueden sin error castigarse como tentativas, porque existen en ellos el carácter de ejecutivos y el peligro actual"[195].

Ahora bien, dadas las características descritas el *phishing*, este habría de ser catalogado como un acto equívoco, por cuanto no siempre podría conducir a la comisión de un delito, por ejemplo, si el *phisher* se conformara solo con la obtención de la información de la víctima sin más ambición que aquella. A mayor abundamiento, como es posible inferir de este trabajo, tampoco es definitivo el delito en específico al cual estarían encaminados los actos realizados por el *phisher*.
Sin perjuicio de lo anterior, el *phishing* podría ser de todas formas perseguido como tentativa de una figura delictual, si se considera que, a pesar de tratarse de un acto equívoco, podría tratarse de uno de carácter contingente, en atención a las condiciones en que tiene lugar el comportamiento.
Así, podría manifestarse de todas formas que se encuentra dirigido a la cometer el delito de estafa, en virtud del carácter fraudulento de las comunicaciones sostenidas con la

[193] Carrara define la tentativa (conato) como "cualquier acto externo que por su naturaleza conduce unívocamente a un resultado criminoso, y que el agente dirige con explícita voluntad a este resultado, pero al cual no le sigue el mismo evento, ni la lesión de un derecho superior o equivalente al que se quería violar". Véase CARRARA, Francesco, *Programa de Derecho Criminal* (Bogotá, Editorial Temis, 1956) I, p. 248.
[194] El acto unívoco es aquel que solo puede conducir a delito. Así se ha manifestado en CURY URZÚA, Enrique, *Tentativa*, cit. (n. 62), p. 44.
[195] CARRARA, Francesco, cit. (n. 193), p. 248.

víctima y aun más, por las diversas ingenierías sociales y subterfugios técnicos que puede emplear para engañar y provocar error en la víctima, a fin lograr su objetivo.
Por otro lado, la conducta llevada a cabo por el *phisher* podría darse en circunstancias en que tomen protagonismo el uso de programas maliciosos para la obtención de la información confidencial, lo cual sería apto para catalogarlo como una "manipulación electrónica" característica del delito de estafa electrónica. De esta forma, sería ostensible que el acto estaría encaminado a obtener el resultado de este delito, es decir, a que posteriormente con los datos obtenido se realice una transferencia no consentida de un activo patrimonial.

2. El *phishing* como delito autónomo

Una tercera posibilidad que se debe considerar es entender el *phishing*, no como acto preparatorio o tentativa en sentido amplio de otros delitos, sino que como un delito autónomo. Para ello, resulta fundamental identificar un bien jurídico que justifique la tipificación independiente de la figura en estudio.

Se debe recordar en este punto que "el legislador considera dañosa una conducta cuando viola un interés. El interés es la posición de un sujeto frente a un bien, y bien es todo aquello que puede satisfacer una necesidad humana, material o ideal. El fin de la norma, y en último término, del derecho todo, es entonces la protección de los intereses"[196]. Así, un "bien jurídico es un bien vital de la comunidad o del individuo, que por su significación social es protegido jurídicamente. La misión del derecho penal es la protección de estos bienes y, como se ha dicho con anterioridad, ese función es precisamente la que le otorga legitimidad para imponer castigos o adoptar medidas de protección"[197].

Tradicionalmente ese bien jurídico con el que se ha vinculado el *phishing* es el patrimonio (presente en delitos como la estafa, el hurto o el robo) y la información propiamente tal (presente en fraudes informáticos).

Cabe destacar que el patrimonio como bien jurídico puede admitir un matiz, por cuanto la doctrina ha optado por diferenciar entre "delitos que afectan los derechos que una persona ejerce respecto de un bien concreto y determinado y aquellos delitos que afectan al conjunto de sus haberes implicando una disminución patrimonial"[198]. Debido a ello, en el caso de la estafa –situado en el ámbito de las defraudaciones– aquello tutelado es el patrimonio como universalidad. En cambio, en delitos como el hurto o el robo, aquello protegido es la propiedad o posesión de las cosas, en tanto existe una relación de carácter fáctico entre una cosa susceptible de avaluación pecuniaria y el sujeto[199]. En este sentido, en los primeros la lesión de un elemento integrante del patrimonio será considerada como

[196] ETCHEBERRY ORTHUSTEGUY, Alfredo, cit. (n. 53), p. 29.
[197] GARRIDO MONTT, Mario, cit. (n. 55), p. 63.
[198] OLIVER CALDERÓN, Guillermo, cit. (n. 95), p. 38.
[199] Así se explica en OLIVER CALDERÓN, Guillermo, cit. (n. 95), p. 38. En este mismo sentido POLITOFF, Sergio; MATUS, Jean Pierre y RAMÍREZ, María Cecilia, cit. (n. 165), p, 299.

tal cuando pueda constatarse una disminución del valor patrimonial considerando al patrimonio en su totalidad. En cambio, en los segundos, basta la lesión al elemento patrimonial para estimarlos consumados, a pesar de que estimado de forma global el patrimonio se mantenga igual[200].

Pues bien, el comportamiento constitutivo de *phishing* puede implicar de variadas formas un peligro patente para este bien jurídico, toda vez que la información confidencial obtenida por el *phisher* está compuesta por datos que –si bien el carácter económico de estos por sí mismos se ha discutido– potencialmente pueden llevar al atacante a realizar actos que vulneren el patrimonio. Tal sería el caso si con ésta información el *phisher* pudiera luego acceder a las cuentas bancarias de la víctima y desde aquella plataforma realizar transferencias electrónicas, ya sea a su propia cuenta o de terceros. Se observaría consecuentemente, una disminución del patrimonio activo de la víctima.

Por otra parte, se ha entendido que "la información ha sido elevada a la categoría de bien jurídico porque ha pasado a ser un interés jurídicamente protegido, que interesa a toda la sociedad"[201]. En esta línea de pensamiento es que la Ley Nº 19.223 entendió como bien jurídico protegido[202] la "calidad, pureza e idoneidad de la información en cuanto tal, contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan"[203]. Así se colige claramente de la Historia de la referida ley, por cuanto se señaló que "con el afán de avanzar en este campo y llenar una laguna presente incluso por los propios jueces-fundadamente, por cierto, pues no se puede aplicar a este tipo de delito la legislación penal común relativa a la estafa-, este proyecto de ley pretende tipificar el delito informático, donde el bien jurídico protegido es la seriedad de la información tratada en forma automatizada, mediante soporte computacional"[204].

En vista de ello, el *phishing* importaría una vulneración de este bien jurídico en virtud de que el *phisher* manipula de manera fraudulenta la información obtenida con el ataque. Asimismo, en aquellos casos en que la forma de ejecución del *phishing* es a través del uso de programas maliciosos o *malware* también se estaría afectando el adecuado uso de la información que se encuentra contenida en un sistema automatizado de datos, toda vez que sin la autorización de los titulares de esta información, esta se ve manipulada para lograr los objetivos del atacante.

No obstante lo anterior, al examinar la conducta descrita en el *phishing*, es posible observar que la obtención por parte del *phisher* de información de carácter confidencial,

---

[200] BALMACEDA HOYOS, Gustavo, *El delito*, cit. (n. 156), p. 15.
[201] SILVA SILVA, Hernán, cit. (n. 154), p. 218.
[202] Esto ha sido criticado, puesto que se postula que el interés digno de protección penal en este tipo de delitos es la confidencialidad del soporte lógico de un sistema automatizado de información. En este sentido, se considera demasiado amplio lo postulado en el proyecto de ley por cuento debiera ser un bien jurídico determinado en términos valorativos, permitiendo evaluar la información por su grado de importancia. Véase con más detalle MOSCOSO ESCOBAR, Romina, cit. (n. 182), p. 16.
[203] ROSENBLUT GORODINSKY, Verónica, cit. (n. 177), p. 258.
[204] BIBLIOTECA DEL CONGRESO NACIONAL, Historia de la ley 19223 "*que tipifica figuras penales relativas a la informática*", p. 24. Disponible en https://www.leychile.cl/Navegar?idNorma=30590

mediante comunicaciones con apariencia de verdaderas, puede significar igualmente un atentado a la intimidad[205] de la víctima del ataque. La intimidad, desde su sentido más natural y obvio, ha de ser entendida como aquella "zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia"[206]. Se debe hacer presente que el ámbito de la intimidad en cuanto parte personalísima y generalmente reservada de los asuntos del individuo, es materia de protección por el derecho[207]. Por cierto, si ya en el complejo mundo actual este espacio de carácter reservado de las personas puede ser objeto de ataques múltiples, los riegos se han ensanchado[208] de manera exponencial con el surgimiento de las nuevas tecnologías[209].

Pues bien, la doctrina ha distinguido distintas perspectivas respecto de la protección de este bien jurídico; una dimensión pasiva, identificable con la facultad del sujeto de rechazar cualquier tipo de intromisión no consentida. Corresponde a una esfera negativa que impone a los terceros una abstención, permitiendo restringir el conocimiento, la información[210]; y una dimensión activa, en la que se actúa con libertad frente a los riesgos de la sociedad tecnológica. Se tienen en tanto facultades de control de los datos de su titular. Se ha hecho referencia a esto último como un poder de disposición sobre los datos[211], permitiendo "decidir cuándo, cómo y bajo qué circunstancias se pueden revelar datos o aspectos de su vida, sus actividades, ideas, reflexiones, actos e información personal"[212].

Se debe tener presente, además, que siguiendo el modelo español, es posible distinguir tres ámbitos de protección al respecto. En primer lugar, se encuentra la intimidad como reducto de la personalidad en la vida privada. Se trata del ámbito tradicional de la intimidad, pudiendo manifestar su negativa a injerencias no deseadas. En segundo lugar, se tiene una intimidad en cuanto confidencialidad o reserva. En tercer lugar, se encuentra

[205] Así se indica en FLORES, Fátima, *Respuesta*, cit. (n. 37), p. 308. En esta misma línea, pero desde una perspectiva un poco más indirecta en SILVA SILVA, Hernán, cit. (n. 154), pp. 217-218.
[206] REAL ACADEMIA ESPAÑOLA, *Diccionario de la lengua española* (Madrid, Grupo Editorial Planeta, 2014), p. 1260.
[207] Así lo describe Goldstein. Asimismo hace referencia a la falta de disposiciones que protejan este ámbito, castigando a quienes lo perturben o atenten contra él. Véase los argumentos de este autor en GOLDSTEIN, Raúl, cit. (n. 158), p. 444.
[208] En efecto, la idea de vida privada, en tanto, ha concitado especial interés a partir del desarrollo de la informática a mediados del siglo XX. Así, el potencial de las herramientas informáticas para recolectar, procesar y analizar información puede poner en riesgo la vida privada de los individuos, lo que ha impulsado hace ya un tiempo las demandas por normas específicas que regulen la recolección y el manejo de información personal. Al respecto LARA, Juan Carlos; PINCHEIRA, Carolina y VERA, Francisco, *La privacidad en el sistema legal chileno*, ONG Derechos Digitales 2014. Disponible en https://www.derechosdigitales.org/tipo_publicacion/publicaciones/
[209] MATA Y MARTÍN, Ricardo, *La protección penal de datos como tutela de las personas*, en *Revista Penal* 18 (2006), p. 218.
[210] Véase su desarrollo en detalle en GARCÍA PINO, Gonzalo, CONTRERAS, Pablo, MARTÍNEZ, Victoria, *Diccionario Constitucional Chileno* (Santiago, Editorial Hueders, 2016), p.328.
[211] MATA Y MARTÍN, Ricardo, cit. (n. 209), p. 220.
[212] GARCÍA PINO, Gonzalo, CONTRERAS, Pablo, MARTÍNEZ, Victoria, cit. (n. 210), p. 329.

una intimidad relacionada con el procesamiento y comunicación de datos a través de las modernas tecnologías de información[213].

Ciertamente, no se vislumbran obstáculos para afirmar que la información confidencial y, en específico, "las claves de acceso y de operaciones bancarias, objetivo inmediato de las conductas de *phishing*, pueden ser consideradas información personal reservada o privada y, por tanto, quedar cubiertas por la intimidad"[214].

Lo dicho, da cuenta de que la conducta realizada en figura del *phishing* engloba por sí sola un desvalor, pues es posible vincularlo directamente con bienes jurídicos protegidos por el ordenamiento, sea por significar un peligro o una efectiva vulneración de los mismos. Ciertamente, el acceso por parte del *phisher* a la información confidencial de la víctima implica ya desde aquel momento una afectación a la intimidad, toda vez que por el engaño inducido por el atacante, la víctima ha actuado con una voluntad viciada y por ende, se ha visto privada del pleno uso de su capacidad de disposición sobre sus datos –pues de conocer las verdaderas circunstancias en que está entregando esta información, lo más seguro es que no lo habría llevado a cabo–. De igual forma, existiría una vulneración de la esfera de su privacidad en aquellos casos en que sin su consentimiento el *phisher* ha tenido acceso a esta información por el uso de programas maliciosos cuyo objetivo es finalmente enviar los datos presentes en el sistema atacado. En tal caso, la víctima ni siquiera ha tenido la oportunidad de rechazar esta intromisión.

Simultáneamente, como ya se ha esbozado, el comportamiento que se realiza en el *phishing* también implica un peligro para el patrimonio de la víctima, pues al tener el *phisher* en su poder la información confidencial de éste, se encuentra en posición de realizar actos que impliquen un menoscabo económico para el atacado.

Bajo esta lógica, es que se ha planteado que los delitos tradicionales tipificadas en nuestro ordenamiento no son capaces de abarcar todo el injusto que comprende la figura del *phishing*[215]. Por ello, se ha sugerido castigo de esta conducta de forma autónoma[216].

A partir de ello es que el *phishing* podría asumir el carácter de delito pluriofensivo; Delito, en tanto desde una perspectiva de la ciencia jurídica se ha definido como "la conducta antijurídica y reprochable, que lesiona el orden social en grado tal de merecer pena"[217]; Pluriofensivo, por cuanto puede afectar a más de un valor o interés a la vez[218], como queda de manifiesto en el análisis anterior, significa no solo un atentado al patrimonio, sino que también a la información misma y a la intimidad.

---

[213] DÍEZ RIPOLLÉS, José, ROMEO CASABONA, Carlos, *Comentarios al Código Penal Parte Especial* (Valencia, Tirant lo Blanch, 2004), p. 692.
[214] FLORES, Fátima, *Respuesta*, cit. (n. 37), p. 315.
[215] Tómese como ejemplo lo dispuesto por la Ley Nº 19.223, en la que se alude al concepto de "dato", el cual podría ser interpretado en términos amplios. Sin embargo, el objeto material se encuentra lejos de abarcar la posible incriminación por la afectación de intereses individuales.
[216] Asimilando en su análisis la figura del *phishing* con el *identity theft* en FLORES, Fátima, *Respuesta*, cit. (n. 37), p. 311. En una línea de pensamiento similar OXMAN, Nicolás, cit. (n. 3), p. 228.
[217] NOVOA, Eduardo, cit. (n. 50), pp.224-227.
[218] Con una idea similar, MOSCOSO ESCOBAR, Romina, cit. (n. 182), p. 17.

III. JUICIO CRÍTICO

Teniendo en cuenta aquello analizado en los apartados precedentes, las siguientes líneas tendrán por objeto tomar una postura respecto de las posibilidades de subsunción para la figura del *phishing.* Para lograr este cometido, se ha optado por analizar las alternativas teniendo como criterio rector aquellos puntos a favor y en contra de cada postura en estudio.

De esta manera, respecto de la posibilidad de que el *phishing* sea considerado como un acto preparatorio, se ha de presentar como un aspecto en contra de esta postura el hecho de que se torne un tanto forzada la calificación de acto preparatorio teniendo como base para ello las teorías clásicas tanto objetivas como subjetivas. Pues, si bien en el apartado correspondiente se ha intentado coincidir el comportamiento característico del *phishing* con los criterios entregados, las tres teorías utilizadas para tal calificación, a saber, la teoría de Beling, la teoría mixta y la teoría pragmática de Carrara, pueden a su vez ser interpretadas desde otra perspectiva obteniendo como consecuencia la clasificación del *phishing* como un acto de ejecución.

En esta misma línea de pensamiento, se debe hacer presente también que la conducta que hemos descrito a lo largo de este trabajo como constitutiva de *phishing*, pareciera que va más allá de un mero acto preparatorio, toda vez que significa no sólo la ordenación de los medios necesarios para asegurar el éxito del ataque, como por ejemplo en la elaboración de los correos electrónicos, sino que implica además la verificación de ciertas acciones concretas, como es la efectiva interacción entre el receptor del mensaje y el *phisher*.

No obstante lo anterior, se debe mencionar que un elemento positivo de esta postura radica en la conveniencia de utilizar como procedimiento para sancionar la configuración de un delito *sui géneris*, toda vez que con ello es posible perseguir penalmente figuras de peligro, adelantando la protección de bienes jurídicos por medio de una tipificación independiente, lo cual en el caso del *phishing* permitiría resguardar intereses valiosos como el patrimonio, la intimidad o la información misma.

Por otro lado, en cuanto a la posibilidad de que el *phishing* sea considerado un supuesto de tentativa en sentido amplio, se debe mencionar como un elemento negativo de esta postura el carácter accesorio de esta última, por cuanto es necesario un vínculo con un delito autónomo determinado. Así las cosas, como ya se ha visto en el análisis realizado en el apartado correspondiente, este aspecto se torna problemático toda vez que la tipificación de los delitos "tradicionales" no cuentan con la flexibilidad necesaria para lograr esta conexión de forma fluida. De esta manera, si bien quizás en el derecho comparado –como en el caso de España– existen figuras que pueden vincularse con el *phishing* de una manera menos problemática, en nuestro ordenamiento jurídico las posibilidades de plantear el castigo del *phishing* a título de tentativa son reducidas. En efecto, aun cuando el delito de estafa se alza como aquel con mayores chances de lograr este cometido, de todas formas ha sido objeto de críticas que hacen dudar de su completa aptitud para sancionar el *phishing* bajo este título. Sucintamente, las críticas han sido dirigidas principalmente a ciertos elementos: respecto de la disposición patrimonial

perjudicial, existiría dificultad en su admisión por la circunstancia de que aquello de lo cual la víctima efectivamente dispone, esto es, el dato personal, por regla general no tendría en sí mismo un valor económico. Quienes plantean esto otorgan como ejemplo aquellos casos en que la víctima entrega al *phisher* su clave de acceso a sus cuentas, con lo cual "no existiría forma de determinar el carácter perjudicial de la disposición"[219]; respecto del engaño, también se ha mencionado que dado el contexto tecnológico actual, en la que la influencia de las tecnologías se ha incluido en la cotidianeidad de la vida en sociedad, no alcanzaría los estándares requeridos (serio, capaz, suficiente) como para constituir la figura[220].

Sin embargo, se debe considerar como un aspecto positivo aquello que a su vez fue criticado respecto de la primera postura, toda vez que pareciera existir mayor claridad al calificar el comportamiento descrito en el *phishing* como un acto de ejecución, utilizando como base las teorías subjetiva limitada, la teoría mixta y la teoría pragmática de Carrara, en directa relación con los posibles delitos con los que podría ser vinculado de ser calificado como un acto constitutivo de tentativa en sentido amplio.

Adicionalmente, el *phishing* parece implicar un injusto menor que determinados delitos, como por ejemplo la estafa o la estafa informática, en tanto aún no existe un perjuicio económico efectivamente apreciable, lo cual se asimilaría de mejor forma a una etapa de ejecución imperfecta de un delito que a un delito plenamente consumando o perfecto.

En cuanto a la tercera posibilidad planteada, esto es, que el *phishing* sea considerado como un delito independiente de carácter pluriofensivo, se presenta como un aspecto negativo el que esta postura pareciera hacer caso omiso a la consideración del derecho penal como *última ratio*. En este sentido, "no siempre es necesario el recurso al Derecho, y en particular al Derecho Penal, para lograr los propósitos de protección de los bienes jurídicos vinculados con ataques relacionados con las TIC"[221]. Junto con ello, se debe ser cauteloso al momento de plantear la inclusión de un tipo específico, puesto que se puede incurrir en un casuismo, dejando sin cobertura conductas dignas de protección, o bien, que luego quede obsoleta la conducta por causa de los constantes avances tecnológicos que se dan en este ámbito.

En relación con lo positivo de esta postura, se destaca el hecho de que recoge un aspecto que las otras posturas no consideran, toda vez que con el *phishing* no solo se pone de manifiesto una amenaza o atentado para un bien jurídico considerado de manera particular, sino que con esta conducta es notorio que son varios los bienes jurídicos en riesgo.

---

[219] ROSENBLUT GORODINSKY, Verónica, cit. (n. 177), p. 258. En este mismo sentido se dice 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" OXMAN, Nicolás, cit. (n. 3), p. 253.

[220] En este orden de ideas, OXMAN, Nicolás, cit. (n. 3), p. 255.

[221] ROMEO CASABONA, Carlos, cit. (n. 2), p. 10.

Habiendo culminado el anterior examen, a juicio de quien escribe, desde una perspectiva de *lege lata* pareciera que la mejor alternativa planteada es calificar el *phishing* como un acto constitutivo de tentativa en sentido amplio del delito de estafa tradicional. Ello debido a que es la figura que coincide de mejor manera tanto respecto de su fase subjetiva como objetiva. Así, a pesar de las críticas mencionadas en su momento, el comportamiento descrito en el *phishing* puede ser identificado fácilmente con los elementos característicos de la estafa, destacando especialmente la existencia de un engaño a partir del empleo por parte del *phisher* de la ingeniería social o subterfugios técnicos. Lo anterior, es perfectamente admisible si hablamos del *phishing* en su modalidad más clásica, es decir, por el envío masivo de correos electrónicos que solicitan la información confidencial.
No obstante, el problema surge al querer perseguir aquellas formas de ejecución de la figura basadas en el uso de un *malware* para la obtención de los datos, puesto que si bien en el derecho comparado pareciera que los modelos han logrado sortear este obstáculo con la creación del delito de estafa electrónica, en nuestro país esta última figura no ha sido tipificada, dejando al descubierto que la legislación vigente en este ámbito es reducida y ampliamente desactualizada. Por lo anterior parece muy forzado e incluso atentatorio para importantes garantías del ámbito del *ius puniendi* (como el principio de legalidad y la consecuente prohibición de analogía), el perseguir penalmente en nuestro país bajo el título de alguno de los delitos de la lay 19.223 estas modalidades de ejecución del *phishing* recientemente aludidas.

En tanto, desde una perspectiva de *lege ferenda*, y directamente relacionado con el último punto mencionado, pareciera necesario que el legislador incluya en nuestro ordenamiento alguna figura nueva en el ámbito del cibercrimen, quizás como un fraude informático, la cual implique un desvalor caracterizado por el uso de las TIC. De esta forma no solo sería posible perseguir penalmente la conducta del *phishing* en la que se emplea un *malware*, sino que también permitiría incluir otros comportamientos que probablemente se desarrollaran a futuro como evolución del mismo.
Así las cosas, se deben realizar ciertas prevenciones bajo este respecto, pues la tipificación que se establezca sebe ser planteada en términos tales que permitan que la conducta se amolde al avance de las nuevas tecnologías, sin dejar de lado los principios limitadores del poder punitivo del Estado.
Quedaría pendiente sin embargo, el otorgar una protección adecuada a esfera de la intimidad de los usuarios de las Redes, por lo que el legislador no debería contentarse con la inclusión de ciertos ciberdelitos, sino que a su vez, debería actualizar la normativa que ampara esta dimensión de las personas, pues a todas luces la tecnología tendrá cada vez más relevancia en todo ámbito en el que el ser humano se desarrolle.

CONCLUSIONES

1. A lo largo las últimas décadas, se ha hecho presente en la cotidianeidad del ciberespacio, una conducta que ha sido denominada por el medio y a la doctrina como "*phishing*". Desde la perspectiva de este trabajo, este ha sido entendido como "aquel comportamiento por el que un sujeto emplea la ingeniería social o subterfugios técnicos para engañar a otro, por medio de comunicaciones aparentemente verdaderas, logrando que este último le remita información de carácter confidencial.

2. Uno de los elementos más característicos de esta figura son la ingeniería social y los subterfugios técnicos, los que ayudan a configurar el carácter aparentemente real de las comunicaciones que recibe la víctima del ataque. De esta forma, se logra que esta última actúe con la convicción de que interactúa con una entidad "visiblemente legítima".

3. Otro elemento especialmente relevante que merece ser destacado es la información de carácter confidencial que es obtenida por el *phisher* como fruto de las comunicaciones con la víctima. La importancia de esta información radica en la potencialidad de afectación de diversas esferas del sujeto que es receptor del ataque, toda vez que pueden verse afectados bienes jurídicos fundamentales como la propiedad y la intimidad.

4. A pesar de que la naturaleza jurídica del *phishing* es incierta, es posible tener en consideración al menos tres posibilidades para tales efectos, a saber, considerarlo un acto preparatorio, una hipótesis de tentativa (en sentido amplio) o un delito independiente.

5. Los principales fundamentos para considerarlo un acto preparatorio se sitúan en la calificación de tal de acuerdo con los criterios provenientes de la teoría de Beling, la teoría mixta, y la teoría pragmática de Carrara. Se completa este análisis al establecer un vínculo con delitos específicos de nuestro ordenamiento jurídico, el robo y el hurto, a cuya comisión estaría dirigida la conducta desarrollada por el *phisher*.

6. Por su parte, los principales argumentos para considerarlo una hipótesis de tentativa (en sentido amplio) radican en que el comportamiento del *phishing* implica, de forma clara, el aprovechamiento de los medios obtenidos de forma previa para el cumplimiento del plan ejecutivo del autor. Reafirman esta consideración los criterios de diversas teorías, entre la que destaca la teoría pragmática de Carrara, la teoría mixta, y las teorías subjetivas. Siendo la tentativa una figura de carácter accesorio, ineludiblemente el examen también ha de referirse a la figuras autónomas con las que se vincularía el *phishing*. Así, se ha intentado establecer una relación con diversos delitos: la estafa, la estafa informática, el hurto y el robo.

7. Por su parte, considerar el *phishing* como un delito independiente se ve justificado en un afán de otorgar la protección debida a importantes bienes jurídicos, entre los que se han identificado la intimidad y el patrimonio. No es baladí hacer hincapié en ello, debido a que la capacidad lesiva de dichos bienes a través de las TIC es potencialmente muy elevada.

BIBLIOGRAFÍA

ANTON ONECA, José, *Las estafas y otros engaños*, en *Nueva Enciclopedia Jurídica*, tomo IX (Barcelona, Editorial Francisco Seix, Barcelona, 1957).

BALMACEDA HOYOS, Gustavo, *El delito de Estafa* (Santiago, Legal Publishing, 2012).

BALMACEDA HOYOS, Gustavo, *El delito de estafa en la jurisprudencia chilena*, en *Revista de Derecho de la Universidad Austral de Chile*, 24 (2011) 1.

BALMACEDA HOYOS, Gustavo, *El delito de estafa informática en el derecho europeo continental*, en *Revista de Derecho y Ciencias Penales* 17 (2011).

BIBLIOTECA DEL CONGRESO NACIONAL disponible en https://www.leychile.cl/Navegar?idNorma=30590&buscar=19223

BIBLIOTECA DEL CONGRESO NACIONAL, Historia de la ley 19223 "*que tipifica figuras penales relativas a la informática*", p. 24. Disponible en https://www.leychile.cl/Navegar?idNorma=30590

BOLETÍN 3009-07 del SENADO DE LA REPÚBLICA DE CHILE, disponible en http://www.senado.cl/appsenado/templates/tramitacion/index.php#

BULLEMORE, Vivian, MACKINNON, John, *Curso de Derecho Penal Parte General* (Santiago, Lexis Nexis, 2007) II.

CARRARA, Francesco, *Programa de Derecho Criminal* (Bogotá, Editorial Temis, 1956) I.

CASTELLS OLIVÁN, Manuel, *The Internet Galaxy: Reflections on the Internet, Business, and Society* (Oxford University Press, Oxford, 2003).

CÓDIGO PENAL ESPAÑOL Y LEGISLACIÓN COMPLEMENTARIA, Disponible en https://boe.es/legislacion/codigos/codigo.php?id=038_Codigo_Penal_y_legislacion_complementaria&modo=1

CREUS, Carlos, *Derecho penal parte especial* (Buenos Aires, Editorial Astrea, 1983).

CURY URZÚA, Enrique, *Derecho Penal Parte General* (Santiago, Ediciones UC, 2011).

CURY URZÚA, Enrique, *Tentativa y delito frustrado: el proceso ejecutivo del delito* (Santiago, Editorial Jurídica de Chile, 1977).

DÍEZ RIPOLLÉS, José, ROMEO CASABONA, Carlos, *Comentarios al Código Penal Parte Especial* (Valencia, Tirant lo Blanch, 2004).

ETCHEBERRY ORTHUSTEGUY, Alfredo, *Derecho Penal Parte General* (Santiago, Editorial Jurídica de Chile, 1998), p. 52.

ETCHEBERRY ORTHUSTEGUY, Alfredo, *Derecho Penal, Parte Especial* (Santiago, Editorial Jurídica de Chile, 1998).

FERNÁNDEZ TERUELO, Javier, *Derecho penal e internet* (Volladolid, Editorial Lex Nova, 2011).

FERNÁNDEZ TERUELO, Javier, *Respuesta penal frente a fraudes cometidos en internet: estafa, estafa informática y los nudos de la red*, en *Revista de Derecho Penal y Criminología* 19 (2007) 2.

FLORES MENDOZA, Fátima, *La responsabilidad penal del denominado mulero o phisher-mule en los fraudes de banca electrónica*, en *Cuadernos de Política Criminal* 110 (2013) 2.

FLORES MENDOZA, Fátima, *Respuesta penal al denominado robo de identidad en las conductas de phishing bancario*, en *Estudios penales y criminológicos* 34 (2014).

GARCÍA PINO, Gonzalo, CONTRERAS, Pablo, MARTÍNEZ, Victoria, *Diccionario Constitucional Chileno* (Santiago, Editorial Hueders, 2016).

GARRIDO MONTT, Mario, *Derecho Penal Parte General* (Santiago, Editorial Jurídica de Chile, 2003).

GOLDSTEIN, Raúl, *Diccionario de derecho penal y criminología* (Buenos Aires, Editorial Astrea, 1983).

HUERTA, Marcelo, *Los delitos de hacking en sus diversas manifestaciones*, en *Revista de Derecho Público de la Agrupación de Abogados de la Contraloría General* 6 (2001).

JAKOBSSON, Markus; MYERS, Steven, *Phishing and Countermesaures:Understanding the Increasing Problem of Electronic Identity Theft* (New Jersey, Wiley, 2007).

LABATUT GLENA, Gustavo, *Derecho penal* (Santiago, Editorial Jurídica de Chile, 1990) I.

LARA, Juan Carlos; PINCHEIRA, Carolina y VERA, Francisco, *La privacidad en el sistema legal chileno*, ONG Derechos Digitales 2014. Disponible en https://www.derechosdigitales.org/tipo_publicacion/publicaciones/

LEE, Wenke, WANG, Cliff, DAGON, David, *Botnet Detection: Countering the Largest Security Threat* (New York, Springer, 2008).

MATA Y MARTÍN, Ricardo, *La protección penal de datos como tutela de las personas*, en *Revista Penal* 18 (2006).

MERA, Jorge, *Hurto y Robo* (Santiago, Lexis Nexis, 2004).

MIRÓ, Fernando, *El Cibercrimen* (Madrid, Marcial Pons, 2012).

MOSCOSO ESCOBAR, Romina, *La ley 19.223 en general y el delito de hacking en particular*, en *Revista Chilena de Derecho y Tecnología* 3 (2014) 1.

NIARCOS, Nicolas, *The Newyorker*. Disponible en http://www.newyorker.com/tech/elements/print-magazine-hackers

NOVOA, Eduardo, *Curso de Derecho Penal Chileno Parte General* (Santiago, Editorial Jurídica de Chile, 2005).

NYKODYM, Nick, KAHLE-PIASECKI, Lisa, ARISS, Sonny, TOUSSAINT, Tracey, *Cibercrime and Business: How to not Get Caught by the Online Phisherman*, en *Journal of International Commercial Law and Technology* 5 (2010) 4.

OLIVER CALDERÓN, Guillermo, *Delitos contra la propiedad* (Santiago, Legal Publishing, 2013).

OXMAN, Nicolás, *Estafas informáticas a través de Internet: acerca de la imputación penal del "phishing" y el "pharming"*, en *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso* 41 (2013) 2.

POLITOFF, Sergio; MATUS, Jean Pierre y RAMÍREZ, María Cecilia, *Lecciones de Derecho Penal chileno, Parte Especial* (Santiago, Editorial jurídica de Chile, 2005).
REAL ACADEMIA ESPAÑOLA, *Diccionario de la lengua española* (Madrid, Grupo Editorial Planeta, 2014).

POLITOFF LIFSCHITZ, Sergio, *Los Actos preparatorios del delito tentativa y frustración: Estudio de dogmática penal y de derecho penal comparado* (Santiago, Editorial Jurídica de Chile, 1999).

ROMEO CASABONA, Carlos, *De los delitos informáticos al cibercrimen. Una aproximación conceptual y político criminal*, en ROMEO CASABONA, Carlos (a cura di), *El Cibercrimen: nuevos retos jurídico-penales, nuevas propuestas jurídico criminales* (Granada, Comares, 2006).

ROSENBLUT GORODINSKY, Verónica, *Punibilidad y tratamiento jurisprudencial de las conductas de phishing y fraude informático*, en *Revista del Ministerio Público* 35 (2008).

RUEDA, María, *Cuestiones político-criminales sobre las conductas de hacking*, en *Derecho penal contemporáneo: Revista Internacional* 28 (2009).

SÁNCHEZ BERNAL, Javier, *El bien jurídico protegido en el delito de estafa informática*, en *Cuadernos del Tomás* 1 (2009).

SENTENCIA ROL 203-2007 6 febrero de 2008 Iltma. Corte de Apelaciones de Arica.

SILVA SILVA, Hernán *Las Estafas* (Santiago, Editorial Jurídica de Chile, 2005).

SRIVASTAVA, Tushar, *Phishing and Pharming- The deadly two* (Boston, Sans Institute, 2007).