Volumen 7, número 1 año 2024
Revista Justicia & Derecho
Recibido el 17 de abril de 2024 / Aprobado el 30 de julio de 2024
Article

El Phishing más allá de la Ley N° 20.009: el riesgo para quien lo controla

Phishing beyond Act 20.009: The Risk for Who Controls It

Iñigo de la Maza Gazmuri[1]

Boris Loayza Mosqueira[2]

RESUMEN

La ley 20.009 regula obligaciones restitutorias e indemnizatorias derivadas del phishing, sin embargo, su alcance se limita a las relaciones de consumo. En este trabajo consideramos la distribución del riesgo entre las partes (el emisor y el usuario) más allá de la ley 20.009, esto es, a partir de lo regulado por ellas en el contrato. Lo que proponemos es que el riesgo debe adjudicarse a quien está en mejor posición de evitarlo. Estimamos que esta opinión resulta consistente con el derecho chileno más allá de su disciplina en la ley 20.009.

Palabras clave: *Phishing – Contratos – Riesgos – Incumplimiento – Depósito irregular*

ABSTRACT

Act 20.009 regulates restitutions and damages caused by phishing, but its scope is confined to consumer relations. In this paper we look beyond this scope and consider risk distribution between parties. We hold that risk should be bear for the party in the best position. We suggest that is opinion this consistent is consistent with Chilean law beyond Act 20.009.

Key words: *Phishing – Contracts – Risk – Breach of contract – Irregular deposit*

[1] Abogado. Licenciado en Ciencias Jurídicas, Universidad Diego Portales, *Master in the Science of Law, The Leland Standford Junior University*. Doctor en Derecho, Universidad Autónoma de Madrid. Profesor titular de Derecho Civil, Universidad Diego Portales, Santiago, Chile.

[2] Abogado. Licenciado en Ciencias Jurídicas y Sociales, Universidad Diego Portales, Santiago, Chile.
Los autores agradecen a Daniela Fuentes Vivar, licenciada en Ciencias Jurídicas y Sociales de la Universidad Diego Portales e integrante de la Academia de Derecho Civil UDP, por su colaboración en la búsqueda y fichaje de sentencias en que se basa esta publicación.

doi: 10.32457/rjyd.v7i1.2525

1. Introducción

La ley 20.009 que establece un Régimen de Limitación de Responsabilidad para Titulares o Usuarios de Tarjetas de Pago y Transacciones Electrónicas en caso de Extravío, Hurto, Robo o Fraude, disciplina, de una forma que ha causado cierta controversia, las obligaciones de restituir e indemnizar derivadas de los fraudes informáticos, entre ellos, el que parece tener mayor relevancia para el sector financiero: el phishing.

En nuestra opinión, el ámbito de aplicación de esa ley se limita a las relaciones de consumo, por lo mismo, más allá de ellas la pregunta acerca de quién soporta los riesgos del phishing debe ser resuelta con cargo al derecho sectorial diverso de dicha ley y al derecho común.

En otro trabajo hemos dado noticia acerca de la fisonomía del phishing y del ámbito de aplicación de la ley 20.009, así como la forma en que esta distribuye los riesgos y las críticas que se le han formulado (De la Maza y Loayza, en prensa). En este trabajo, nuestra intención consiste en examinar cómo se distribuye el riesgo más allá de la disciplina de la ley 20.009, esto es, a partir de lo regulado por ellas en el contrato. Nuestro propósito no es, por tanto, analizar el régimen legal, sino, en cambio, revisar la forma en que, fuera de la 20.009, se distribuyen las consecuencias del phishing.

Procedemos de la siguiente manera. En primer lugar, damos cuenta de qué entendemos por phishing. En segundo lugar, ilustramos, a través de un ejemplo extraído de una reciente sentencia de la Corte de Apelaciones de Santiago, la situación que nos interesa en este artículo y planteamos la pregunta sobre la distribución de los riesgos causados por el phishing. En tercer lugar, prestamos atención a la primera respuesta que, sin contar la regulación específica (nos referimos, por supuesto, a la ley 20.009), dio un sector de la doctrina a esta cuestión y que fue empleada por los tribunales superiores de justicia: la disciplina del depósito irregular. A continuación, en cuarto lugar, procuramos demostrar que la solución se encuentra en otro lado, a saber, en el contrato que vincula a las partes debidamente integrado por la regulación sectorial. Con este objeto, examinamos algunas sentencias que nos aproximan a esta solución. En quinto lugar, desarrollamos esta idea mostrando un modelo de distribución de riesgos presente en el derecho estadounidense, advirtiendo su conformidad con la regulación sectorial y con ciertas sentencias de nuestros tribunales superiores de justicia. Finalmente, en sexto lugar, establecemos la forma en que el riesgo del phishing debe ser distribuido más allá de la ley 20.009.

2. ¿Qué es el phishing?

Según el *Legal Information Institute* de la Universidad de Cornell, el phishing se define como "a type of computer and internet fraud that involves the creation of false digital resources intended to resemble those of legitimate business entities, such as a website or email, and dissemination of seemingly legitimate digital correspondence that leads back to those false resources via email or URL to induce individuals to reveal or disclose sensitive, personally identifying information."[3]1

Algo semejante se encuentra en nuestro derecho. Así, por ejemplo, Nicolás Oxman señala que el "'phishing' es la pesca de datos personales a través de Internet. Ahora bien, ella puede constituir una modalidad de estafa informática, si tiene lugar a través del envío masivo de correos electrónicos con enlaces a páginas 'web' falsas, respecto de las cuales se imita el contenido o la imagen de un determinada

[3] 1 Disponible en https://www.law.cornell.edu/wex/phishing. En el mismo sentido, aunque de manera más sintética, la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, lo define como la "captación de datos mediante suplantación de identidad".

entidad financiera o bancaria para engañar al destinatario del mensaje, logrando así sustraer la información personal que posibilita el acceso a sus cuentas de débito personal. De este modo, se logra la consumación de un perjuicio patrimonial mediante el retiro de dinero o, bien, directamente a través de operaciones de compras no consentidas por Internet" (Oxman, 2013, pp. 216-217). Por su parte, Laura Mayer y Guillermo Oliver exponen que "el *phishing* implica una obtención fraudulenta de datos de identidad personales de clientes de bancos y de sus cuentas bancarias o tarjetas de crédito, orientada a ejecutar transacciones electrónicas a favor del agente o de terceros". Y, luego añaden que "Desde un punto de vista terminológico, el *phishing* evoca la 'pesca' de información o el intento de que las eventuales víctimas 'muerdan el anzuelo' y proporcionen (consciente o inconscientemente) los datos que busca el hechor. En tanto supone emplear información personal ajena, el *phishing* usualmente es vinculado con el concepto de hurto o robo de identidad (también conocido como *identity theft*)" (Mayer y Oliver, 2020, pp. 156-157). Ambas definiciones enfatizan los aspectos relevantes de esta clase de ilícito, de un lado, la finalidad del phishing (esto es, el engaño al titular de los datos) y, de otro lado, su carácter fraudulento.

Pues bien, siendo las cosas de este modo, lo que acá entendemos por phishing es la captación de datos confidenciales de manera ilícita y sin el consentimiento del titular de dichos datos.

3. Un ejemplo ilustrativo y la distribución del riesgo[4]

El representante legal de una empresa intenta acceder, a través de su computador personal, al sitio web de su institución bancaria con la finalidad de efectuar una serie de transferencias a sus proveedores desde la cuenta corriente de su representada. La página web del banco es capturada por una "página de seguridad" que solicitó la clave de seguridad del cliente para continuar. Esta fue digitada en al menos tres ocasiones; en todas ellas, la página arrojó error. Al ingresar con un usuario diferente, el cliente advierte la existencia de diez transferencias bancarias no autorizadas por un monto total de $50.000.000; frente a esto, solicita al banco la restitución de los montos extraídos de su cuenta. El banco se niega argumentando que las transacciones se efectuaron a través del sitio seguro de internet, sin transgredir sus sistemas de seguridad (infraestructura y/o equipos). Se interpone un recurso de protección al considerar que el actuar del banco es arbitrario e ilegal, el que fue acogido por la Corte de Apelaciones de Santiago, quien consideró que el Banco no había cumplido con el procedimiento establecido en la ley 20.009, y lo condenó a restituir la suma de dinero.

[4] Se trata de la sentencia de Corte de Apelaciones de Santiago, de 26 de mayo de 2023. Distribuidora de Materiales de Construcción S.A.C. con Banco de Chile (2023).

Por razones que expusimos en otro trabajo, la sentencia nos parece errónea: en este caso no se aplicaba la ley 20.009, pues no existía una relación de consumo.[5,6] Sin embargo, el ejemplo nos sirve para ilustrar un caso de phishing, toda vez que el cuentacorrentista entrega sus datos confidenciales necesarios para realizar la transacción a un tercero que lo engaña y que los utiliza para obtener dinero de la cuenta corriente. El caso, además, presta utilidad para formular la cuestión que nos interesa. Un tercero ha girado $50.000.000 de la cuenta corriente de la víctima, por supuesto esta tiene acciones en contra del tercero, sin embargo, lo más probable es que no pueda ubicarlo, de manera que, generalmente, la cuestión será si puede dirigirse por esa restitución en contra de quien ejecutó la orden de pago (en este caso, el banco).

Si la respuesta es afirmativa, el riesgo del phishing lo soporta el banco; si la respuesta es negativa, el riesgo del phishing lo soporta el dueño de los fondos (en este caso, el cuentacorrentista) quien, de una parte, no podrá obtener la restitución de su dinero y, de otra parte, deberá cargar con los daños que esto le cause.

[5] Estimamos que la ley 20.009 no recibe aplicación en un caso como este, pues esta se limita a las relaciones de consumo. Es decir, su ámbito de aplicación está determinado a las relaciones entre un consumidor y un proveedor en los términos de la Ley N° 19.496 sobre Protección de los Derechos de los Consumidores (en adelante, "LPDC"). Nos permitimos, con todo, resumir apretadamente los argumentos expuestos en otro lugar (De la Maza y Loayza, en prensa).
En primer lugar, la ley 20.009 emplea la expresión "usuario" sin definirla; sin embargo, dicho concepto tiene un ámbito perfectamente establecido en la LPDC, la que dispone una relación de sinonimia con el concepto "consumidor" en su artículo 1 N° 1. Y, teniendo en cuenta el artículo 20 del Código Civil, no es posible asignarle a la expresión un significado diferente al que ya tiene.
En segundo lugar, los artículos 5 y 6 de ley 20.009 remiten explícitamente a las normas de la LPDC. Así, el primero señala "El procedimiento para ejercer esta acción será el establecido en los Párrafos 1° y 2° del Título IV de la ley N° 19.496, sobre protección de los derechos de los consumidores", mientras que el segundo precepto dispone "Los emisores, operadores comercios y otros establecimientos afiliados a un sistema de tarjetas de pago, así como las demás entidades que intervengan o presten servicios asociados a pagos y transacciones electrónicas, u otros sistemas de características similares, incluyendo los proveedores de servicios de iniciación de pagos, deberán adoptar las medidas de seguridad necesarias para prevenir la comisión de los ilícitos descritos en esta ley y el resguardo de la privacidad de los datos de los titulares o usuarios de medios de pago conforme a la legislación y normativa que les resulte aplicable, y velarán por la prestación segura del respectivo servicio en los términos señalados por el artículo 23 de la ley N° 19.496".
En tercer lugar, tanto la historia fidedigna de las leyes 20.009, 21.234 y la reciente 21.673 dejan en claro que su ámbito de aplicación es una relación de consumo; esto es, su *ratio legis* es la tutela de los consumidores o usuarios del sistema financiero.
Finalmente, lo mismo ha sido resuelto por la jurisprudencia y afirmado por la doctrina. Así, por ejemplo, en un caso resuelto por la Corte de Apelaciones de Talca, se señaló lo siguiente:
"Que, en concordancia con la norma precitada se desprende claramente que, si bien la ley publicada difiere del proyecto de ley original, la finalidad de la ley es brindar una mayor protección a los consumidores de los bancos en el caso de sufrir fraudes financieros de los que no pueden tener conocimiento hasta que el dinero ha sido utilizado o sustraído de sus productos bancarios, siendo uno de los métodos más utilizados para esto el llamado 'phishing', método que se vale del uso de correos electrónicos o sitios web especialmente confeccionados para otorgar apariencia de legitimidad simulando la marca o presencia en línea de un banco o institución financiera, y de esta forma, obtener del titular los datos necesarios para la realización de operaciones bancarias, como lo que ha sucedido en el caso de autos" (en Troncoso con Banco de Chile (2021)).
Por su parte, tratándose de los autores, María José Arancibia ha señalado: "No obstante existir este estatuto de protección, como lo es la Ley del Consumidor, se hacía necesario un estatuto especial, por cuando la LPDC se basa en el cumplimiento de un determinado estándar de cuidado o diligencia del banco, pero no establece de manera clara el contenido de esta diligencia o cuidado, punto determinante para el efecto de lograr configurar un régimen objetivo de distribución de riesgos que permita proteger al cliente bancario"; y, más adelante, añade: "Como puede apreciarse, la Ley N° 20.009 nace con el claro espíritu de proteger al tarjetahabiente estableciendo una presunción simplemente legal a su favor, cuando ha realizado un uso normal y correcto de la tarjeta de crédito. Por esta razón, debe descartarse una interpretación, como la que en su oportunidad sostuvieron los asesores de las instituciones financieras, quienes propendían a que fuera el tarjetahabiente quien se encontrara en la obligación de asumir los perjuicios derivados del extravío de la tarjeta y que solo una vez efectuado el aviso se podía exigir la responsabilidad del organismo emisor, pues ello más que incentivar el cuidado y la correcta conservación y seguridad de la tarjeta de crédito, termina por crear un régimen donde la diligencia que emplea el cliente en el cuidado de su tarjeta termina siendo irrelevante, quedando en definitiva esta obligación de custodia subsumida dentro de la carga de dar aviso de la pérdida: así, de seguirse una interpretación que imposibilite la responsabilidad de la entidad bancaria antes del aviso, nos encontraríamos con que no existe deber alguno de custodia de la tarjeta y que el cliente en consecuencia debería responder incluso de los casos que escapan del deber de diligencia y cuidado que le son exigidos en virtud de la relación contractual" (Arancibia, 2017, pp. 140 y 142).

[6] Cabe tener presente que, si bien la ley 20.009 se limita a las relaciones de consumo, en los términos de la Ley N° 20.416 que fija normas especiales para las empresas de menor tamaño, también ha de tenerse por consumidores a ciertas empresas de menor tamaño (Momberg, 2013, pp. 13-16). En este sentido, Munita y Aedo sostienen que "el estatuto del consumo resulta de igual forma aplicable a las personas jurídicas que integran la categoría Pyme, las que, desde luego, pueden revestir la calidad de clientes bancarios y eventualmente ser afectadas por el fraude" (Munita y Aedo, 2020, p. 101). Lo mismo se encuentra en Arancibia, 2021, p. 219.

4. La cuestión del depósito irregular

Las normas de la ley 20.009 únicamente se aplican cuando existe una relación de consumo y, si sucede de esta manera, las reglas especiales de dicha ley prefieren a las del derecho común y a las de la LPDC.[7] Si, en cambio, no se trata de una relación de consumo —esto es, si, como en el caso de la sentencia antes descrita, se trata de dos empresas—, no recibe aplicación ni la ley 20.009 ni la LPDC. Lo que recibe aplicación es el derecho común.

En un primer momento, y con alguna frecuencia, los tribunales superiores de justicia se han servido del depósito irregular[8] para distribuir los riesgos del phishing.[9] Es más, en alguna ocasión se ha señalado que es la tesis predominante de los tribunales (Cordero y Contardo, 2020). No pretendemos tratar exhaustivamente el uso que los tribunales han dado a esta figura, sino que procuramos ilustrarlo a través de algunos ejemplos.

Un primer ejemplo se encuentra en un fallo de la Corte de Apelaciones de Concepción, de fecha 6 de agosto de 2019.[10] En este, el tribunal sostuvo que, al negarse a restituir los fondos sustraídos, el actuar del banco fue ilegal y arbitrario, pues, ante un fraude informático en el uso de las claves de una cuenta corriente y productos asociados a ellas, no era posible sostener que los dineros sustraídos sin el consentimiento del cliente correspondan a caudales específicos de éste, ya que "los depósitos de dinero en las entidades financieras se realizan como un simple género y no como especies o cuerpos ciertos, a lo que debe sumarse el carácter de bienes fungibles de las especies monetarias empleadas para la satisfacción de lo debido, conforme dispone el artículo 575 del Código Civil, esto es, dotadas de igual poder liberatorio". Por lo mismo, en opinión de la Corte, el único afectado por el engaño era, en su calidad de propietario de los fondos, el banco recurrido, quien debía adoptar todas las medidas de seguridad necesarias para proteger adecuadamente el dinero bajo su resguardo.

El segundo ejemplo se extrae de una sentencia resuelta, también a propósito de un recurso de protección, por la Corte de Apelaciones de Iquique, de 30 de diciembre de 2019.[11] Según este tribunal, las instituciones bancarias celebran contratos de depósito irregular con los clientes, pues aquello que se deposita es una suma de dinero que no está destinada a mantenerse en arca cerrada, presumiendo que se permite su empleo, obligando al depositario a la restitución de una igual cantidad.

---

7 Por supuesto, solo en lo que resultan especiales respecto de la LPDC. Así, por ejemplo, si se trata de una relación de consumo, recibirá aplicación preferente la ley 20.009, pero la LPDC se seguirá aplicando en aquello no dispuesto por la ley 20.009. De esta manera, si en el contrato que disciplina el medio de pago existen cláusulas exonerativas de responsabilidad, su carácter abusivo debe discutirse con cargo a la LPDC.

8 Sobre el depósito irregular: Guzmán Brito, 2014, pp. 87-137.

9 Véase, por ejemplo, Troncoso con Banco Scotiabank Chile (2021); Ayala con Banco Scotiabank Chile (2021); Requena con Banco Scotiabank (2020); Davagnino con Scotiabank Chile (2020); Millar con Banco Scotiabank Chile S.A. (2020); Comercializadora y Distribuidora Mauricio Lainez Rojas E.I.R.L. con Banco de Chile (2020); Ruiz con Banco de Chile (2020); Cañas con Banco Scotiabank Chile (2020); Muñoz con Banco del Estado de Chile (2020); Alviña con Banco de Chile (2019); De Lima con Banco del Estado de Chile (2019); Valdés con Sardon (2020) y Zúñiga con Itaú Corpbanca S.A. (2020).

10 Ramírez con Banco de Chile (2019).

11 Palma con Banco de Chile (2019). En lo que interesa, la sentencia dispone "(…) tal como razona el considerando sexto de la sentencia citada: 'Ante un fraude informático en el uso de las claves de una cuenta corriente y productos asociados a ellas, no resulta posible sostener que los dineros sustraídos, sin el consentimiento del cliente, correspondan a caudales específicos de éste, toda vez que los depósitos de dinero en las entidades financieras se realizan como un simple género y en caso alguno como especies o cuerpos ciertos, a lo que debe sumarse el carácter de bienes fungibles que en su esencia representan las especies monetarias empleadas para la satisfacción de lo debido, conforme dispone el artículo 575 del Código Civil, esto es, dotadas de igual poder liberatorio, y por cuya razón pueden reemplazarse unas a otras mutua o recíprocamente en la ejecución de las obligaciones sin perjuicio ni reclamo del acreedor (Carlos Ducci Claro, Derecho Civil, Parte General, Editorial Jurídica de Chile, 1980)'". En el mismo sentido: Péndola con Banco Scotiabank (2023).

En fin, el tercer ejemplo se halla en un fallo de 25 de mayo de 2020, nuevamente sobre un recurso de protección, conocido esta vez por la Corte de Apelaciones de Temuco.[12] Conforme se lee en la sentencia es el banco el propietario de los fondos y, por lo mismo, sobre este recae el deber de eficaz custodia material de estos, debiendo adoptar, al efecto, todas las medidas de seguridad necesarias para proteger adecuadamente el dinero bajo su resguardo. Señala el tribunal:

"Que por tales motivos, aun cuando el fraude informático se haya ejecutado mediante el uso irregular de los datos y claves bancarias personales de la empresa recurrente, lo sustraído es dinero, bien fungible, con lo que resulta no solo jurídica sino físicamente imposible sostener y menos acreditar la exacta identidad de las especies sustraídas mediante el fraude perpetrado, circunstancia que lleva a concluir que en definitiva el único afectado por el engaño referido es el banco recurrido, dada su calidad de propietario del dinero depositado (…)".

Un sector de la doctrina nacional ha manifestado simpatía con esta solución. Así, por ejemplo, en una columna de prensa de 29 de mayo de 2019, Hernán Corral señala que:

"Aunque el contrato de cuenta corriente tiene su especialidad, sin duda se funda en esta misma lógica: el cuentacorrentista 'deposita' dinero en la cuenta, el banco se hace dueño del mismo y se compromete a restituir el valor a requerimiento del titular de la cuenta.

Siendo el banco deudor de un género que no perece, no puede excusarse por la pérdida de la cosa ni siquiera, aunque fuera fortuita (arts. 1510 y 1670 CC).

En el caso, el dinero fue extraído por un tercero de manera fraudulenta, pero siendo una cosa fungible esa pérdida no puede ser atribuida a una cuenta en particular, aunque se hubiera hecho uso de la información de esta para lograr la extracción. La pérdida debe imputarse al patrimonio general del banco, al igual que si un estafador se hiciera pasar por un cliente del banco e imitando su firma obtuviera que el banco le entregara dinero en billetes. Sería absurdo que el banco pretendiera que ha sido el cliente el afectado por la sustracción y que por ello no restituirá los fondos que este tenía en su cuenta" (Corral, 2019; Alvear, 2019).

Por su parte, algunos años después, Renzo Munita explica algo semejante en base a los siguientes dos argumentos:

"El primero de ellos se refiere a la naturaleza del contrato sobre el que se traba la litis. Cabe recordar, y de hecho la sentencia lo hace, que para establecer la identidad jurídica del contrato de cuenta corriente bancaria habrá que visualizar el de depósito, vínculo definido en el artículo 2211 Código Civil, y que se encuentra recogido en el artículo 40 de la ley general de bancos. Si bien la primera de las normas se refiere a la obligación del depositario de guardar y de restituir en especie aquella cosa corporal objeto del contrato, la naturaleza del bien depositado, el dinero, implica liberar al depositario de la obligación de restituir exactamente el mismo bien. Dicha obligación solo existiría si el depósito de dinero fuera en arca cerrada, cuya llave la tuviera el depositante, o con otras precauciones que hagan imposible tomarlo sin fractura (a la luz del art. 2221 CC en relación con el art. 2228 CC), cuestión que no se da en los hechos. De aquí que el banco no sea mero tenedor del dinero, sino que dueño de éste, en atención a que el contrato celebrado representa un título traslaticio de dominio; algo similar sucede con el cuasi usufructuario. El depósito, es entonces, de naturaleza irregular.

(…)

[12] Cabrera con Banco del Estado de Chile (2020).

Con base en lo mencionado, el segundo argumento se refiere a la participación del bien sustraído en una especial clasificación de cosa fungible y, en consecuencia, con vocación a confundirse con otros bienes de idéntica nomenclatura, que como dijimos, una vez depositado por el cuentacorrentista ingresa en propiedad al patrimonio del banco. De aquí que el art. 575 CC ordene: 'Las especies monetarias en cuanto perecen para el que las emplea como tales, son cosas fungibles'. Luego, el dinero sale del patrimonio del cliente con motivo del contrato e ingresa en el del banco. Así, el desvío fraudulento, de afectar a un patrimonio, aquel no es otro que el de aquella entidad, sin que a su vez éste se libere de su obligación de restituir la suma equivalente de dinero depositado" (Munita, 2023, pp. 293-294).

En el mismo sentido, Feliciano Tomarelli también considera que la tesis del depósito irregular es la más adecuada, sin embargo, añade que, bajo ciertas circunstancias, el riesgo pertenece al usuario (Tomarelli, 2020, pp. 1051-1052). En sus palabras:

"(…) el banco podría imputar al cuentacorrentista los daños causados por el acto criminal del tercero que accede fraudulentamente a la cuenta corriente, cuando el depositante haya sido negligente en el cuidado de sus claves de acceso, generando o aumentando el riesgo de la ocurrencia de la acción intencional del tercero. En esos casos, nos parece necesario que la acción del tercero no haya podido haber tenido éxito sin culpa del depositante (su negligencia es la que habilita al tercero a sustraer los fondos) y que los daños que sufra el banco hayan sido previsibles en el caso concreto" (Tomarelli, 2020, pp. 1060-1061).[13]

Su conclusión al respecto es que, no obstante la acción que del banco en contra de quien accede fraudulentamente a los depósitos, este podría solicitar la indemnización de perjuicios contra el depositante, en la medida en que este (el cliente) haya sido negligente en el cuidado o manejo de sus claves personales, creando o aumentando el riesgo de ser víctima de fraude, siendo previsible para un hombre medio puesto en las mismas circunstancias (Tomarelli, 2020, p. 1062).

Otro sector de la doctrina mantiene una opinión diversa, crítica del uso que los tribunales han dado a la figura del depósito irregular en estos casos. Javier Rodríguez, por ejemplo, advierte que el hecho de que la conducta del cliente sea indiferente al momento de distribuir los riesgos del fraude bancario, hace que la solución descrita sea más insostenible cuando más evidente es la falta de cuidado del cuentacorrentista (Rodríguez, 2019, p. 196). Y, luego, añade:

"nadie duda que el cuentacorrentista tiene un crédito contra el banco, que consiste en una obligación genérica, y que el banco no puede eximirse de cumplir con su obligación por la pérdida de objetos que correspondan a dicho género. Sin embargo, es igualmente cierto que en el phishing no se verifica el perecimiento de especies monetarias que son de propiedad del banco. Por lo mismo, las normas generales del depósito irregular relativas al perecimiento de objetos depositados resultan inaplicables para determinar la atribución del riesgo en caso de fraude bancario" (Rodríguez, 2019, p. 200).

Enseguida, el autor estima que se trata de un problema de distribución de riesgos, en los siguientes términos:

[13] En una línea similar, María José Arancibia explica que la distinción entre depósito regular e irregular es sumamente interesante y aplicable al tema de los fraudes bancarios, pues "como consecuencia de un fraude en transacciones electrónicas se originan cargos, abonos, o giros de dinero en cuentas corrientes bancarias, cuentas de depósitos a la vista, cuentas de provisión de fondos de un determinado titular. Es por ello que existen buenas razones para imputar en primer término dicho riesgo a los bancos, quienes son titulares del dinero depositado. Lo mismo ocurre, aunque de manera mucho más evidente, cuando se trata de un fraude que afecta los fondos incluidos dentro de las líneas de crédito" (Arancibia, 2021, pp. 223-224).

"(…) las normas sobre el riesgo de pérdida de las especies entregadas en el depósito irregular no ofrecen una solución al problema de los fraudes informáticos, desde que en este último caso no tiene lugar la pérdida de especies monetarias determinadas de propiedad del deudor. El núcleo del problema del fraude bancario estriba en la suplantación de la persona del deudor. En este contexto, en lugar de fijar una atribución objetiva de responsabilidad —como se desprende con claridad del fallo bajo análisis— corresponde evaluar los riesgos que entrañan las transferencias de fondos, determinar quién está en posición para evitarlos y, sobre la base de esto, fijar deberes de cuidado a cada parte, sea legal o contractualmente.

Si bien el problema del phishing es relativamente reciente, es posible encontrar normas para un problema análogo, como es la falsificación del cheque: en principio, la pérdida asociada al cobro de un cheque falsificado será de cargo del cuentacorrentista, ya que él debe cuidar su chequera; sin embargo, al banco le corresponde verificar, entre otras circunstancias, que la firma no sea visiblemente disconforme, por lo que será este quien responda en caso de no cumplir con este deber. De esta forma, se establece una distribución del riesgo atendiendo a los deberes de cuidado que cabe exigir de cada parte. La solución es más equitativa que hacer responder siempre al banco sobre la base de la existencia de una obligación de género con el cuentacorrentista" (Rodríguez, 2019, p. 201).

He ahí las opiniones encontradas en la doctrina con relación al depósito irregular. Según creemos la solución correcta se encuentra más cerca de las ideas de Rodríguez, más adelante explicaremos por qué; ahora mismo, prestará utilidad presentar algunas sentencias de los tribunales superiores que nos permitan acopiar material para nuestra respuesta.

5. Algunas sentencias más recientes

Las sentencias más recientes de los tribunales superiores de justicia parecen haber abandonado la tesis del depósito irregular (Fernández y Labra, 2023, p. 733); como sostiene Javier Rodríguez: "La jurisprudencia reciente se ha inclinado decididamente por un análisis subjetivo, en el que las consecuencias asociadas a la calificación de la cuenta corriente como un depósito irregular han pasado a un segundo plano, mientras que el elemento clave para resolver está dado por la observancia del banco de una conducta adecuada a la regulación sectorial vigente, así como el nivel de cuidado del cliente en el manejo de sus datos personales" (Rodríguez, 2019, pp. 196-197).

Más adelante y a propósito del grado de diligencia con que deben comportarse las partes, el autor continúa señalando que la distribución del riesgo se establece en atención a los deberes de cuidado que caben exigirles a las partes. De este modo, la solución sería más equitativa que responsabilizar siempre al banco sobre la base de una obligación de género con el cuentacorrentista (Rodríguez, 2019, p. 201).

Una vez más, no pretendemos dar cuenta exhaustiva del estado de las cosas en tribunales, pero una búsqueda concienzuda de las bases de datos pertinentes arroja varias sentencias en este sentido. Así, por ejemplo, la Corte Suprema ha resuelto que las instituciones financieras tienen una obligación de control y monitoreo, siendo la conducta normal del cliente un elemento de juicio que los debe ayudar a advertir una conducta engañosa. Así, en un fallo de 14 de agosto de 2019,[14] sostuvo: "Que, teniendo presente los hechos asentados resulta que se advierte que la operación cuestionada se realizó a través de la página web oficial del banco recurrido y fuera del espacio habitual de operaciones del cliente, lo que permite descartar

[14] Alviña con Banco de Chile (2091). En el mismo sentido, Maluk con Banco de Chile (2020).

que los hechos se han debido única e inequívocamente a una actividad dolosa o negligente de su parte. Además, las obligaciones de monitoreo y control de fraudes recaen expresamente en la institución recurrida, donde los patrones de conducta del cliente son elementos de juicio para la determinación de una operación engañosa, cuestión que no fue informada en detalle por el Banco recurrido. Sobre la institución bancaria recae la obligación de vigilancia y el análisis de la correlación de eventos y seguridad de las operaciones, por lo que, una vista general de las operaciones del cliente en la cuenta corriente respectiva otorga verosimilitud a la intervención de terceros en los sistemas de seguridad que otorgó la recurrida".

La misma Corte, en un fallo de 10 de junio de 2020,[15] se pronuncia sobre el deber de cuidado de un banco tratándose de un cuentacorrentista que es una persona jurídica. Para el tribunal, esta circunstancia le otorga atributos diversos a los que habitualmente se observan en una cuenta corriente personal, ya que se adecúan a las necesidades de una empresa, permitiéndoles "programar y autorizar varias operaciones en forma simultánea, con un límite en el monto de la operación sustancialmente mayor a los que se prevén para las personas naturales, en los que se deben aportar los datos del apoderado autorizado, para luego proceder a agendar, inscribir y autorizar las operaciones dubitadas". Esto, unido al uso de diversas IP para efectuar las transacciones y al monto de las mismas permiten atenuar el rigor de las obligaciones de vigilancia, análisis de la correlación de eventos y seguridad de las operaciones que pesan sobre la institución bancaria.

En una tercera sentencia, pronunciada el 20 de enero de 2021[16] por la Corte Suprema, en que se realizaron una serie de operaciones a través de la página web del banco recurrido, la Corte señala lo siguiente:

"Que, de lo expuesto, se concluye que la recurrida se limitó a señalar en su informe que la transferencia se realizó utilizando la clave del cliente. Sin embargo, no acreditó de modo alguno que la operación objetada, se haya realizado desde el computador o algún dispositivo de uso personal de éste; por consiguiente, el banco recurrido no ha podido excepcionarse de cubrir las pérdidas sufridas por el recurrente, dado que no acreditó, estando en posición de hacerlo, que el siniestro haya ocurrido con ocasión de la sustracción de las claves por parte de terceros por una vía distinta a la obtención de las mismas a través de su página web oficial.

(…)

Además, las obligaciones de monitoreo y control de fraudes recaen expresamente en la institución recurrida, donde los patrones de conducta del cliente son elementos de juicio para la determinación de una operación engañosa, cuestión que no fue informada en detalle por el Banco recurrido. Sobre la institución bancaria recae la obligación de vigilancia y el análisis de la correlación de eventos y seguridad de las operaciones, por lo que, una vista general de las operaciones del cliente en la cuenta corriente respectiva otorga verosimilitud a la intervención de terceros en los sistemas de seguridad que otorgó la recurrida".

Por lo que toca a las cortes de apelaciones, en un fallo de 26 de junio de 2020, pronunciado por la Corte de Apelaciones de Concepción,[17] se desprende la existencia de obligaciones de "monitoreo" y "control de fraudes" que recaen en las instituciones bancarias, donde los patrones de conducta de los clientes son elementos que permiten la determinación de una operación engañosa.[18] Se lee en el fallo:

[15] Comercial Piña Espina y Cía. Ltda. con Banco de Chile (2020).

[16] Gutiérrez con Scotiabank Chile (2021).

[17] Jaureguiberry con Banco Scotiabank de Chile (2020).

[18] Lo mismo se presenta en Meza con Scotiabank Chile S.A. (2020), donde se añade que "es responsabilidad del Banco enviar una alerta de fraude al usuario, identificando las operaciones sospechosas, con constancia de su recepción por parte del cliente".

"Sobre la institución bancaria recae la obligación de vigilancia y el análisis de la correlación de eventos y seguridad de las operaciones, por lo que, una vista general de las operaciones de la cliente en la cuenta corriente respectiva, otorgan verosimilitud a la posible intervención de terceros en los sistemas de seguridad que otorgó la recurrida".

De manera semejante se encuentra una sentencia de 13 de diciembre de 2021, dictada por la Corte de Apelaciones de San Miguel;[19] según se lee en el considerando décimo tercero, son los bancos los que deben contar con sistemas o procedimientos que permitan identificar, evaluar, monitorear y detectar en el menor tiempo posible operaciones de fraude, de modo de abortar las actividades fraudulentas, lo cual debe realizarse en función de los estándares de protección que actualmente exige la industria. A continuación, en el considerando décimo sexto, sostiene que es responsabilidad del banco:

"(…) asegurar al consumidor final la seguridad en el acceso y uso de los canales y medios dispuestos en virtud del contrato de servicios celebrado y que dicha obligación no se limita solo al envío de notificaciones, avisos generales o disposición de advertencias vía mecanismos de transparencia activa del Banco. En efecto el estándar que la ley precitada exige, en virtud de la naturaleza de las obligaciones que rigen la relación contractual entre las partes debe alcanzar la inviolabilidad de todos aquellos medios dispuestos para la comunicación del cliente con su banco, debiendo contar con sistemas o protocolos que permitan identificar, evaluar, monitorear y detectar preventivamente, o en el menor tiempo posible, aquellas operaciones con patrones de fraude, de modo de identificar, marcar y abortar operaciones potencialmente fraudulentas".

Más recientemente, en una sentencia de 6 de enero de 2023, la Corte de Apelaciones de Santiago resuelve que el phishing queda fuera de la esfera de control del Banco.[20] En su considerando cuarto se expresa: "Que, en este contexto, debe recordarse que el demandante ha señalado no haber sido él quien realizó los pagos objetados. Sin embargo, no se ha aportado a los autos antecedente alguno que dé cuenta cierta de esa circunstancia, esto es, que no fue él, sino una tercera persona quien, por sí y sin el consentimiento del actor, realizó fraudulentamente los pagos indicados en la demanda a través de la plataforma de Servipag S.A., vulnerando los sistemas de seguridad dispuestos por el Banco demandado. Antes por el contrario, en la propia demanda se afirma que el dispositivo Digipass del actor se encontraba en su poder el día de la operación y que, desde hacía un tiempo que venía operando con el sistema Mi Pass a través de su teléfono celular; a lo que cabe agregar la consideración de que las probanzas referidas en el fundamento anterior dan cuenta de que el banco, por su parte, sí había dado cumplimiento a su deber de prestar seguridad, puesto que proveyó al demandante con un sistema de precisamente seguridad para operar en sus canales de autoatención, mediante la digitación, para acceder a ellos, de su RUT, un PIN y una tercera clave de seguridad dispensada por el dispositivo Digipass que al efecto le otorgó cuya custodia asumió bajo su exclusiva responsabilidad; el que entrega periódicamente claves diversas a las que solo puede tener acceso quien lo posea. Además, aparece de aquellos antecedentes, apreciados conforme a las máximas de la experiencia, que el banco demandado permanentemente entrega a sus clientes, por diversas vías, recomendaciones de seguridad en la utilización de sus canales de auto atención. Por último, también dicha documentación permite concluir que la entidad demandada tenía a disposición de sus clientes y recomendaba el uso del software de seguridad Rapport de Trusteer, que el actor, sin embargo, no había descargado al día 7 de septiembre de 2018".

[19] Arriaza con Banco Scotiabank (2021).

[20] Luna Zurita con Banco de Chile (2023).

Un razonamiento similar se encuentra en un fallo pronunciado el 8 de mayo de 2023 por la misma Corte de Apelaciones de Santiago;[21] según se desprende del fallo, casos como el que motivan este trabajo (phishing) sobrepasan la esfera de cuidado de los bancos, consistente en diversas medidas o sistemas de seguridad, pues provienen del actuar del usuario, por lo que no es posible hacerlos responsables.

En fin, el mismo tribunal, pero en una sentencia de 8 de junio de 2023[22] declara que para determinar la responsabilidad del banco se debe revisar si el ardid (phishing) sobrepasó la esfera de cuidado que el banco debió otorgar —a través de sus protocolos de seguridad— o, si, por el contrario, por no cumplir con dicho deber se pudo concretar el fraude. Se lee en el fallo: "Que en tales condiciones, no existen antecedentes que permitan atribuir responsabilidad infraccional en los hechos investigados al banco reclamado y que llevaron a las transferencias no consentida de dinero desde la cuenta de la denunciante y, por lo mismo, nada conduce a hacerle soportar al banco la responsabilidad de este hecho; pues conforme la manera en que se verificó el acto fraudulento denunciado, según fue establecido, no consta que el banco haya incumplido las normas antes referidas, por cuanto la defraudación sufrida por el denunciante, no se produjo por una insuficiencia de las medidas de seguridad del demandado, ni se acreditó vulneración de sus sistemas de seguridad. Por el contrario, aparece que la actividad fraudulenta excedió los límites de los protocolos y controles a que está obligado el Banco, pues otorgando todos los medios de seguridad para este tipo de transferencias al denunciante, esto es, clave de acceso a la página web, tarjeta de coordenadas y una tercera clave de validación que se envía a un teléfono previamente registrado, terceros obtuvieron mediante 'phishing' los datos de la querellante".

Lleva, entonces, razón Javier Rodríguez: las sentencias más recientes han abandonado la tesis del depósito irregular y, en cambio, han prestado atención a la situación del usuario como a la de quien ejecuta la orden de pago, atendiendo desde la legislación sectorial a los deberes de cuidado de este último y, con cargo al derecho común, han considerado el deber de cuidado de los usuarios.

Según diremos a continuación, el escenario es uno en el que, tendencialmente al menos, el riesgo se asigna a quien está en mejores condiciones de controlarlo.

6. El riesgo para quien lo controla[23]

6.1. Del depósito irregular al contrato

Como ya se ha visto, un sector de la doctrina nacional se ha servido de la figura del depósito irregular para administrar la distribución del riesgo del phishing. Uno de sus exponentes, sin embargo, añade que dicha figura debe compaginarse de alguna manera con la conducta que observe el usuario, y acude, para justificar su opinión, a los *enabling torts* (Tomarelli, 2020, pp. 1058-1059).[24]

[21] Banco del Estado de Chile con José Luis Rocco Tachi Red de Suministros Eléctricos EIRL (2023)

[22] Simunovic con Banco Santander Chile S.A. (2023).

[23] Se trata de una idea antigua que puede rastrearse en Calabresi, 1984, pp. 143-144 y Hirschoff y Calabressi, 1972, p. 1060. Recientemente se ha empleado para considerar la cuestión de los pagos indebidos en Gilboa y Kaplan, 2022, pp. 61-89.

[24] Sostiene Tomarelli que "En el derecho anglosajón, se han analizado casos como el que tratamos bajo la noción de *enabling torts*, que alude a los *torts* en donde existen al menos dos conductas que están causalmente conectadas con el daño generado, y que una de ellas habilitó o "pavimentó el camino" para que la segunda tuviera lugar (y se causara el daño), sin que existiera un concierto previo. Sin embargo, no todos los casos son iguales, y es necesario hacer distinciones. De suyo, la distinción primordial que han hecho los tribunales norteamericanos en las últimas décadas es entre *superseding causes* e *intervening forces*". Sobre los *enabling torts* puede consultarse, Rabien, 1999, pp. 435-454.

Nosotros estamos de acuerdo en que, cualquiera que sea el rendimiento del depósito irregular para justificar la cuestión de la distribución del riesgo del phishing, este debe condecirse con algún otro antecedente que permita tener en cuenta la conducta del usuario, sin embargo, a diferencia de Tomarelli, no tomamos ese antecedente de la responsabilidad extracontractual (Tomarelli, 2020, pp. 1061-1062), sino de la contractual.[25]

Existiendo contrato (es decir, en la gran mayoría de los casos) las partes pueden asignar el riesgo como lo estimen conveniente, pues, en los casos que motivan el presente trabajo —esto es, entre un usuario "empresa" y una institución financiera— están más allá de la LPDC y, por lo tanto, de las cláusulas abusivas; aunque, por supuesto, es posible que un tribunal estime que la distribución del riesgo que explícitamente hace el contrato es contraria a la costumbre, a la buena fe, el orden público o algo semejante.[26] Sin embargo, al menos en las decisiones de los tribunales chilenos, no hemos encontrado que se discuta específicamente acerca de estas cláusulas, por lo tanto, nuestro análisis, de una parte, asume la existencia de un contrato y, de otra, que ese contrato no ha distribuido explícitamente el riesgo del phishing.

Desplazados hacia el contrato, el problema de los riesgos del phishing debe administrarse a través de la disciplina del incumplimiento y los remedios. Por otra parte, el recurso al incumplimiento exige determinar el contenido de la prestación que se estima como incumplida. Según estimamos, con independencia del tipo de contrato que vincule al emisor[27] con el usuario,[28] para que se presenten los problemas que el phishing ha causado en el ámbito nacional, ha de ser el caso que exista un contrato entre el emisor y el usuario en virtud del cual el emisor se obligue a poner dinero a disposición del usuario o terceros en virtud de la autorización del usuario, en términos tales que si no lo hiciera —es decir, si no pusiera dicho dinero a disposición de un tercero— incumpliría con su obligación.[29]

A continuación, la pregunta es ¿cuándo debe estimarse que la orden fue autorizada por el usuario? Dos supuestos no son controversiales: el primero tiene lugar si el mismo usuario autoriza; el segundo es si el usuario encarga a alguien ejecutar las conductas en que consiste la aceptación.

El supuesto controversial, en cambio, es el phishing. Convendrá considerar por qué debemos estimarlo como controversial a este respecto. En un sentido, resulta evidente que el usuario no ha autorizado el pago; nunca fue su intención cuando entregó su información comercial al tercero que lo engañó. Sin embargo, desde la perspectiva del contrato, no resulta evidente que la autorización exija la intención del usuario.

La razón es la siguiente: generalmente (al menos en los casos de phishing que han resuelto los tribunales nacionales), dicha autorización funciona, por así decirlo, de manera "ficta",[30] es decir, a través de la ejecución de un procedimiento de seguridad destinado a autenticar al usuario mediante el uso de cierta información confidencial que controla el usuario (el ejemplo por antonomasia es el "digipass" o la "tarjeta de coordenadas").

---

25 Asumir las cosas de esta manera involucra una limitación que conviene constatar: la existencia de un contrato. Somos conscientes de que pueden existir supuestos en que quien pone a disposición el dinero no se encuentra vinculado contractualmente con el usuario y, en esos casos, la responsabilidad será extracontractual y deberá construirse, parcialmente al menos, a través de la regulación sectorial que consideraremos más adelante. Sin embargo, nos parece que, aun en ese supuesto, el riesgo seguirá siendo de quien está en mejores condiciones de controlarlo.

26 Sobre el uso de estos criterios más allá de la LPDC, ver: Campos, Munita y Pereira, 2022, pp. 187-217.

27 Aquí y en adelante, denominamos "emisor" a cualquiera que se obligue contractualmente a ejecutar órdenes de pago a través de ciertas instrucciones cuyo control se ha asignado al usuario.

28 Sobre los tipos de contratos, véase: Arancibia, 2017 y, en menor medida, Arancibia, 2021.

29 Ver artículo 89 de la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) N.º 1093/2010 y se deroga la Directiva 2007/64/CE.

30 Algo semejante a lo que, tratándose de la tradición, dispone el artículo 684 del Código Civil.

Tratándose del tipo de phishing sobre el que predominantemente han resuelto los tribunales chilenos, al cual podemos denominar "*spear phishing*",[31] en virtud de un engaño, un tercero adquiere del usuario la información necesaria para ejecutar el procedimiento de seguridad y, ejecutado, el emisor pone el dinero a disposición de alguien distinto al usuario. Según nuestra impresión, descontada la responsabilidad civil del tercero (el que engañó al usuario para que suministrara la información confidencial necesaria para solicitar la orden de pago), la distribución del riesgo entre el usuario y el emisor no depende de las normas del depósito irregular, sino de que haya existido o no un incumplimiento contractual por parte del emisor.

Entendemos que existirá incumplimiento contractual cuando el emisor pone a disposición el dinero en condiciones distintas a las pactadas. De esta manera, la cuestión clave parece ser el contenido de ese pacto y para determinar ese contenido no solo debe estarse al acuerdo explícito de las partes, sino que, en virtud del artículo 1546 del Código Civil, a su integración a través de la regulación sectorial (Guzmán, 2002, pp. 11-23 y Campos, 2021, pp.105-159).

Según estimamos, si ese pacto no adjudica explícitamente el riesgo del phishing, dicha adjudicación exige prestar atención a la situación del emisor y del usuario, y advertir que el fraude puede tener lugar por actuaciones en contra del emisor o en contra del usuario. Tendencialmente, son el emisor y el usuario quienes están en mejores condiciones de controlar su propio riesgo, por lo mismo, en principio al menos, el riesgo debe asignárseles de esa manera.

Volveremos sobre las consecuencias de esto al presentar un modelo de distribución de los riesgos del phishing en la última parte de este artículo, por ahora, nos interesa advertir que, en nuestra opinión, esta forma de adjudicar el riesgo del phishing resulta consistente tanto con la regulación sectorial como con las sentencias que hemos presentado más arriba, no obstante, antes de consultar ambas nos interesa mostrar cómo funciona la adjudicación del riesgo en el ámbito estadounidense. Creemos que esto presenta interés, pues ha existido un vigoroso desarrollo de la materia que puede resultar útil para llenar algunas cuestiones pendientes en el ámbito nacional.

6.2. El artículo 4 A del Uniform Commercial Code

El artículo 4 A del *Uniform Commercial Code* (en adelante, "UCC") asigna el riesgo de fraudes en las operaciones de pago de un banco.[32]

Comienza con la sección 4A-204 (a) cuyo texto, en lo relevante, es el siguiente:

"If a receiving bank accepts a payment order issued in the name of its customer as sender which is (i) not authorized and not effective as the order of the customer under Section 4A-202, or (ii) not enforceable, in whole or in part, against the customer under Section 4A-203, the bank shall refund any payment of

[31] Existen múltiples variedades de phishing; en otro trabajo señalamos lo siguiente: "el phishing puede manifestarse de formas diversas. Así, por ejemplo, el más común es denominado "spear phishing" y va dirigido a individuos específicos respecto de los cuales se cuenta con alguna información y de quienes se procura, a través del engaño, otra de carácter confidencial, ya sea a través de mensajería, correos electrónicos, solicitando la descarga de malware, spyware, etc. Cuando el canal de comunicación es el teléfono, se denomina vishing ("voice phishing") y si se trata de un mensaje de texto toma el nombre de "smishing". Cuando lo que se utiliza son post en medios sociales se trata de "Angler Phishing". Si se utiliza una falsa red de wifi, se conoce como "evil twin phishing" Se denomina "email phishing" a un tipo de mail en el que se suplanta la dirección del remitente y "HTTPS phishing" cuando lo que se falsifica es un sitio web y "pharming" cuando a través de un software malicioso se dirige al usuario a un sitio web falsificado. Se denomina "pop-up phishing" cuando aparece un aviso de seguridad en el computador que sugiere bajar un programa que, a su turno instala malware en el computador o que dirige a un centro de soporte falsificado" (De la Maza y Loayza, en prensa).

[32] Seguimos aquí la exposición de Haley, 2015. También se puede consultar a Turner, 1994.

the payment order received from the customer to the extent the bank is not entitled to enforce payment (…)". [33]

Como se ve, en primer lugar, el banco es responsable si la orden de pago no es eficaz según las normas del mandato (*agency*). Sin embargo, tratándose de órdenes emitidas por medios electrónicos, no será frecuente que se apliquen estas normas. La razón es que el mecanismo de autenticación (claves, coordenadas, etc.) impide al banco saber quién está ordenando el pago. Por lo tanto, en la mayoría de los casos, la defensa del banco será la excepción contenida en la Sección 4A-202 (b), según la cual:

"If a bank and its customer have agreed that the authenticity of payment orders issued to the bank in the name of the customer as sender will be verified pursuant to a security procedure, a payment order received by the receiving bank is effective as the order of the customer, whether or not authorized, if (i) the security procedure is a commercially reasonable method of providing security against unauthorized payment orders, and (ii) the bank proves that it accepted the payment order in good faith and in compliance with the security procedure and any written agreement or instruction of the customer restricting acceptance of payment orders in the name of the customer. The bank is not required to follow an instruction that violates a written agreement with the customer or notice of which is not received at a time and in a manner affording the bank a reasonable opportunity to act on it before the payment order is accepted". [34]

[33] "Si un banco acepta una orden de pago emitida en nombre de su cliente, como remitente, que: (i) no está autorizada y no es efectiva como la orden del cliente según la sección 4A-202, o (ii) no es ejecutable, en su totalidad o en parte, contra el cliente según la sección 4A-203, el banco reembolsará cualquier pago efectuado a nombre del cliente, en la medida en que el banco no tenga derecho a ejecutar el pago", traducción de los autores.

[34] "Si un banco y su cliente han acordado que la autenticidad de las órdenes de pago emitidas al banco a nombre del cliente como remitente serán verificadas de acuerdo con un procedimiento de seguridad, una orden de pago recibida por el banco receptor es efectiva, si está autorizado o no, si (i) el procedimiento de seguridad es un método comercialmente razonable para proporcionar seguridad contra órdenes de pago no autorizadas, y (ii) el banco demuestra que aceptó la orden de pago de buena fe y de conformidad con el procedimiento de seguridad y cualquier acuerdo o instrucción escrita del cliente que restrinja la aceptación de órdenes de pago a nombre del cliente. El banco no está obligado a seguir una instrucción que viole un acuerdo escrito con el cliente o notificación de que no se recibe a la vez y de una manera que ofrece al banco una oportunidad razonable para actuar sobre ella antes de que se acepte la orden de pago", traducción de los autores.

De esta manera, aun si la orden de pago no fue autorizada, el banco podrá excepcionarse si acredita que existió un procedimiento de seguridad[35] conocido por el cliente, comercialmente razonable[36] y que, de buena fe, [37] aceptó el pago en conformidad a dicho procedimiento.

Con todo, la Sección 4A-203(a) (1) permite al cliente recobrar el monto aun si se satisfacen los requisitos del párrafo anterior —y en lo que interesa aquí— bajo las siguientes circunstancias:

"The receiving bank is not entitled to enforce or retain payment of the payment order if the customer proves that the order was not caused, directly or indirectly, by a person (i) entrusted at any time with duties to act for the customer with respect to payment orders or the security procedure, or (ii) who obtained access to transmitting facilities of the customer or who obtained, from a source controlled by the customer and without authority of the receiving bank, information facilitating breach of the security procedure, regardless of how the information was obtained or whether the customer was at fault. Information includes any access device, computer software, or the like". [38]

[35] Definido en la Sección 4ª-201 en los siguientes términos: "Security procedure" means a procedure established by agreement of a customer and a receiving bank for the purpose of (i) verifying that a payment order or communication amending or cancelling a payment order is that of the customer, or (ii) detecting error in the transmission or content of the payment order or communication. A security procedure may require the use of algorithms or other codes, identifying words or numbers, encryption, callback procedures, or similar security devices. Comparison of a signature on a payment order or communication with an authorized specimen signature of the customer is not by itself a security procedure".
"'Procedimiento de seguridad': procedimiento establecido por acuerdo entre un cliente y un banco receptor con el fin de (i) verificar que una orden de pago o una comunicación que modifica o cancela una orden de pago es la del cliente, o (ii) detectar errores en la transmisión o el contenido de la orden de pago o la comunicación. Un procedimiento de seguridad puede requerir el uso de algoritmos u otros códigos, la identificación de palabras o números, cifrado, procedimientos de devolución de llamada o dispositivos de seguridad similares. La comparación de una firma en una orden de pago o comunicación con un modelo autorizado de firma del cliente no es por sí misma un procedimiento de seguridad", traducción de los autores, traducción de los autores.

[36] La Sección 4ª-202(c) establece un test de razonabilidad comercial en los siguientes términos: "Commercial reasonableness of a security procedure is a question of law to be determined by considering the wishes of the customer expressed to the bank, the circumstances of the customer known to the bank, including the size, type, and frequency of payment orders normally issued by the customer to the bank, alternative security procedures offered to the customer, and security procedures in general use by customers and receiving banks similarly situated. A security procedure is deemed to be commercially reasonable if (i) the security procedure was chosen by the customer after the bank offered, and the customer refused, a security procedure that was commercially reasonable for that customer, and (ii) the customer expressly agreed in writing to be bound by any payment order, whether or not authorized, issued in its name and accepted by the bank in compliance with the security procedure chosen by the customer".
"Razonabilidad comercial de un procedimiento de seguridad es una cuestión de derecho que debe determinarse teniendo en cuenta los deseos del cliente expresados al banco, las circunstancias del cliente conocido por el banco, incluyendo el tamaño, tipo, y la frecuencia de las órdenes de pago normalmente emitidas por el cliente al banco, los procedimientos de seguridad alternativos ofrecidos al cliente y los procedimientos de seguridad de uso general por los clientes y los bancos receptores situados de manera similar. Un procedimiento de seguridad se considera comercialmente razonable si (i) el procedimiento de seguridad fue elegido por el cliente después de que el banco ofreció, y el cliente se negó, un procedimiento de seguridad que era comercialmente razonable para ese cliente, y (ii) El cliente ha aceptado expresamente por escrito cualquier orden de pago, autorizada o no, emitida en su nombre y aceptada por el banco en cumplimiento del procedimiento de seguridad elegido por el cliente", traducción de los autores.

[37] Sobre la buena fe, véase a Haley, 2015, pp. 140-141, quien señala lo siguiente: "While the case law on this issue is limited, the most important consideration appears to be whether the fraudulent transactions are markedly different from the bank customer's normal wire transfer activity. In Experi-Metal, the court was influenced by the large number of fraudulent transactions over a short period of time, which was a distinctive departure from the customer's normal wire transfer activity. In contrast, the Choice Escrow court noted that the wire transfer was not so irregular as to have caused suspicion. However, other irregularities, such as the ultimate destination of the funds or the recipient of the funds, should be considered in the analysis as well".
"Si bien la jurisprudencia sobre esta cuestión es limitada, la consideración más importante parece ser si las transacciones fraudulentas son notablemente diferentes de la actividad normal de transferencia bancaria del cliente bancario. En Experi-Metal, el tribunal se vio influenciado por el gran número de transacciones fraudulentas durante un corto período de tiempo, que fue un distintivo de la actividad normal de transferencia bancaria del cliente. En contraste, el tribunal de Choice Escrow señaló que la transferencia bancaria no era tan irregular como para haber causado sospechas. Sin embargo, en el análisis también deben tenerse en cuenta otras irregularidades, como el destino final de los fondos o el receptor de los fondos", traducción de los autores.

[38] "El banco receptor no tiene derecho a ejecutar o retener el pago de la orden de pago si el cliente demuestra que el pedido no fue causado, directa o indirectamente, por una persona (i) encargado en cualquier momento de actuar por el cliente con respecto a las órdenes de pago o el procedimiento de seguridad, o (ii) que obtuvo acceso a las instalaciones de transmisión del cliente o que obtuvo, de una fuente controlada por el cliente y sin autorización del banco receptor, información que facilite el incumplimiento del procedimiento de seguridad, independientemente de cómo se obtuvo la información o si el cliente era culpable. La información incluye cualquier dispositivo de acceso, software de computadora o similar", traducción de los autores.

La excepción tiene lugar cuando la orden de pago no tuvo su causa directa o indirecta en dependientes del cliente o personas que han obtenido acceso a los equipos del cliente o que han obtenido información de una fuente controlada por el cliente. Se trata de casos en los cuales el problema de seguridad no afecta de ninguna manera al cliente, sino al banco. Según señala Haley, en estos casos, la litigación es escasa pues los bancos prefieren pagar (Haley, 2015, p. 101).

Así las cosas, aun cuando el procedimiento de seguridad se haya observado escrupulosamente, el cliente podrá recuperar el monto del pago si prueba que no fue causado directa o indirectamente por alguien de quien sea responsable.

Pues bien, el modelo es el siguiente: frente a una orden de pago respecto de la que el cliente alegue la restitución de los fondos, el banco se encuentra obligado salvo que: (1) haya sido ejecutada por un mandatario del cliente, o (2) que se haya realizado ejecutando el procedimiento de seguridad acordado entre el banco y el cliente, y el banco haya sido suficientemente cuidadoso al ejecutar la orden. Pero, aun en este último caso, el banco deberá responder si el problema de seguridad que permitió la orden de pago no autorizada lo afectó a él y no al cliente; es decir, si el problema queda dentro de su esfera de protección y no en la del cliente.

Según creemos, este modelo es consistente con la regulación sectorial y las decisiones de los tribunales superiores de justicia.

6.3. Regulación sectorial y sentencias

Por lo que toca a la regulación sectorial, se puede acudir acá a la normativa dictada por la Superintendencia de Bancos e Instituciones Financieras y al Banco Central. Así, en primer lugar, el Capítulo 1-7 de la Recopilación Actualizada de Normas de Bancos e Instituciones Financieras (RAN) que regula la "Transferencia electrónica de información y fondos", establece, entre los requisitos que deben cumplir los bancos para los sistemas de pago utilizados, lo siguiente:

"C) El sistema debe proveer un perfil de seguridad que garantice que las operaciones sólo puedan ser realizadas por personas debidamente autorizadas para ello, debiendo resguardar, además, la privacidad o confidencialidad de la información transmitida o procesada por ese medio.

Los procedimientos deberán impedir que tanto el originador como el destinatario, en su caso, desconozcan la autoría de las transacciones o mensajes y la conformidad de su recepción, debiendo utilizarse métodos de autentificación para el acceso al sistema y al tipo de operación, que permitan asegurar su autenticidad e integridad.

La institución financiera debe mantener permanentemente abierto y disponible un canal de comunicación que permita al usuario ejecutar o solicitar el bloqueo de cualquier operación que intente efectuarse utilizando sus medios de acceso o claves de autenticación. Cada sistema que opere en línea y en tiempo real, debe permitir dicho bloqueo también en tiempo real.

(…)

H) Los bancos deberán ponderar la exposición al riesgo financiero y operativo de los sistemas de transferencia de que se trata y considerar, en consecuencia, las instancias internas de revisiones y autorizaciones previas que sean necesarias.

Para el adecuado control de los riesgos inherentes a la utilización de estos sistemas, es necesario que los bancos cuenten con profesionales capacitados para evaluarlos antes de su liberación y para mantener bajo vigilancia, mediante procedimientos de auditoría acordes con la tecnología utilizada, su funcionamiento, mantención y necesidades de adecuación de los diversos controles computacionales y administrativos que aseguran su confiabilidad".

Asimismo, tratándose de transferencias electrónicas entre clientes de distintos bancos, se exige que los canales electrónicos que ofrezcan las instituciones bancarias para realizar estas transferencias cuenten con privilegios de autorización adecuados y medidas de autentificación, controles de acceso lógico y físicos, infraestructura de seguridad para observar el cumplimiento de las restricciones y límites que se establezcan para las actividades internas y externas.

Finalmente, respecto de la prevención de fraudes entre clientes interbancarios, la normativa indica:

"Los bancos deberán contar con sistemas o procedimientos que permitan identificar, evaluar, monitorear y detectar en el menor tiempo posible aquellas operaciones con patrones de fraude, de modo de marcar o abortar actividades u operaciones potencialmente fraudulentas, para lo cual deberán establecer y mantener, de acuerdo a la dinámica de los fraudes, patrones conocidos de estos y comportamientos que no estén asociados al cliente.

Estos sistemas o mecanismos deberán permitir tener una vista integral y oportuna de las operaciones del cliente, del no cliente (por ejemplo, en los intentos de acceso), de los puntos de acceso (por ejemplo, direcciones IP, Cajero Automático u otros), hacer el seguimiento y correlacionar eventos y/o fraudes a objeto de detectar otros fraudes, puntos en que estos se cometen, modus operandi, y puntos de compromisos, entre otros".

En segundo lugar, si ahora se considera el Capítulo III.J.1 sobre "Emisión de tarjetas de pago" emitido por el Banco Central, se advierte que los emisores "deberán disponer de resguardos operacionales y de seguridad adecuados en función de las tarjetas que emitan, conforme a los estándares y mejores prácticas internacionales sobre medios de pago. Como mínimo, deberán contar con una tecnología de seguridad que permita proteger apropiadamente la información contenida en las tarjetas, implementar mecanismos robustos de autentificación y prevención de fraudes, así como facilitar la verificación oportuna de la disponibilidad de cupos y saldos de éstas, y su bloqueo, según corresponda".

Y dentro de las políticas que deben adoptar se hallan "las medidas de ciberseguridad y otra índole adoptadas para prevenir y mitigar los riesgos de fraude".

Por otra parte, tanto en el contrato entre los emisores y la entidad afiliada como aquel entre los emisores y los operadores se exige pactar medidas de seguridad.

Más adelante, la normativa sectorial establece que "Los bancos deben instruir a los tarjetahabientes acerca de las precauciones que deben tener en el manejo de sus tarjetas físicas y de los medios en que ellas pueden ser utilizadas, especialmente para mantener en resguardo las claves personales, así como de las principales normas que rigen su uso". Y se añade que los bancos deberán disponer de canales 24 al día para permitir a los usuarios denunciar pérdida, robo, adulteración o falsificación de las tarjetas.

En tercer lugar, el Capítulo 8-41 de la RAN que regula las "Tarjetas de Pago" establece que las tarjetas "deben contar con una tecnología de seguridad que permita proteger apropiadamente la información contenida en las tarjetas de pago, implementar mecanismos robustos de autentificación y prevención de

fraudes, así como facilitar la verificación oportuna de la disponibilidad de cupos y saldos de éstas, y su bloqueo, según corresponda".

En cuarto lugar, se encuentra la Circular N° 40 sobre "Normas generales para empresas emisoras y operadoras de tarjetas de crédito", que establece la misma obligación del párrafo anterior, detallándola.

En fin, en quinto lugar, la Ley N° 20.950 que "Autoriza emisión y operación de medios de pago con provisión de fondo por entidades no bancarias" establece, en su artículo 1, que los medios de pago deben cumplir con "los estándares y condiciones mínimas en materias de seguridad, fiabilidad, aceptabilidad, uso, masividad, entre otras, que el Banco Central de Chile establezca por norma general".

Como puede verse, la regulación sectorial exige seguridad a los bancos tanto respecto del soporte como de la operación (es decir, la autenticación en la orden de pago) y el monitoreo y control de fraudes.

Ahora bien, en lo que concierne a las sentencias, ya se ha dado noticia de ellas, ahora se trata de advertir si son consistentes con el modelo del artículo 4A del UCC y la normativa sectorial. Por lo que se refiere a las sentencias de la Corte Suprema, la de 14 de agosto de 2019 y la del 20 de enero de 2021, como se recordará, exigen al emisor actividades de monitoreo de fraudes; la de 10 de junio de 2020 exige un grado de diligencia tanto el emisor como al usuario.

Por su parte, si se presta atención a las sentencias de las Cortes de Apelaciones citadas más arriba, la del 28 de julio de 2020 exige al emisor cumplir con deberes de seguridad, la del 13 de diciembre de 2021 le exige monitorear operaciones previas con patrones de fraude y las sentencias de 6 de enero, 8 de junio y 8 de mayo, todas de 2023 fallan consistentemente que si el fraude (en este caso, phishing) no fue gracias a un incumplimiento de la medidas de seguridad a que se encuentra obligado el emisor, este no debe restituir.

6.4. Las medidas de seguridad

Al examinar tanto el artículo 4A del UCC como la normativa sectorial y las sentencias de los tribunales superiores de justicia, aparecen, consistentemente, ciertas medidas de seguridad a las que el emisor es obligado.

Esas medidas de seguridad asumen una fisonomía diversa. Acaso las más evidentes se refieran, en primer lugar, a los equipos e instalaciones del emisor que le permiten efectuar las órdenes de pago. Así, por ejemplo, el Capítulo III.J.1 sobre "Emisión de tarjetas de pago", exige que las entidades afiliadas a los sistemas cuenten con dispositivos electrónicos, informáticos o de otra naturaleza que operen con captura en línea de las transacciones, permitiendo que los montos de dinero asociados a éstas sean inmediatamente cargados en la línea de crédito o en la cuenta del titular o usuario de la tarjeta respectiva.

Junto a ellas, en segundo lugar, los mecanismos de autenticación (claves, dispositivos, etc.) deben, en el lenguaje del artículo 4A del UCC, ser "comercialmente razonables", es decir, deben ser suficientemente seguros. Lo anterior se manifiesta, por ejemplo, en la Circular N° 40 sobre "Normas generales para empresas emisoras y operadoras de tarjetas de crédito", la cual exige que los procedimientos de resguardo contemplen la homologación y certificación de dispositivos y terminales, mecanismos *anti-tamper* (es decir, la captura de datos del cliente), la capacidad de encriptación de información sensible, etc.

En tercer lugar, existe otra manifestación de las medidas de seguridad a las que, en el derecho chileno, se encuentra obligado el emisor: la obligación de monitoreo. De este modo, con cargo a la "buena fe", al artículo 4A del UCC, a la regulación sectorial y a las sentencias de los tribunales superiores de justicia,

el emisor debe monitorear y detectar las operaciones con patrones de fraude. Así, por ejemplo, la misma Circular N° 40 impone controles de seguridad físicos y lógicos, como accesos debidamente autorizados, autenticación de los usuarios, además de una apropiada configuración de las redes, uso de firewalls, y las herramientas de detección de intrusos. Por otra parte, señala que las empresas deben contar con sistemas que les permitan advertir la presencia de transacciones irregulares y reacciones de manera oportuna, mediante procedimientos de bloqueo de información de los clientes.

En un sentido similar, la ley 20.009 también exige, en su artículo 4°, que los emisores adopten estándares mínimos de seguridad, registro y autenticación, esto es, las medidas de seguridad necesarias para prevenir la comisión de los ilícitos y la privacidad de los usuarios de medios de pago. Exige, también, que las medidas de seguridad cuenten con sistemas de monitoreo que tengan como objetivo detectar las operaciones no habituales del usuario, implementar procedimientos internos para gestionar las alertas que generan los sistemas de monitoreo, identificar los patrones de fraude, establecer límites y controles en los canales de atención[39]. Si bien es cierto que, en los casos que interesan a este trabajo, la ley 20.009 no resulta procedente, la norma permite advertir cierto estándar en la exigencia de dichas medidas de seguridad.

En fin, estas cuestiones también han sido anotadas por la doctrina. María José Arancibia ha indicado respecto de las obligaciones del emisor, que este: "deberá contar con ciertas medidas de seguridad como mínimo, como son el contar con sistemas de monitoreo que tengan como objetivo detectar aquellas operaciones que no corresponden al comportamiento habitual del usuario; implementar procedimientos internos para gestionar las alertas generadas por dichos sistemas de monitoreo; identificar patrones de potenciales fraudes, conforme a las prácticas de la industria y recomendaciones, los que deberán incorporarse al sistema de monitoreo de operaciones; y establecer límites y controles en los diversos canales de atención que permitan mitigar las pérdidas por fraude. Estos límites y controles deberán basarse en consideraciones de riesgo objetivas, generales y no discriminatorias, en relación con la naturaleza del medio de pago y la clase de operaciones que permita efectuar, y su supervisión queda entregada al órgano fiscalizados competente. La falta o deficiencia de tales medidas será considerada para la determinación de las responsabilidades correspondientes a cada uno de ellos, que pudiere perseguir en su contra el usuario u otro afectado" (Arancibia, 2021, p. 221).

7. El modelo de distribución de riesgo

Acopiado el material anterior, creemos que, en aquellos casos en los que no recibe aplicación la ley 20.009 —esto es, cuando no exista relación de consumo—, el modelo de distribución del riesgo causado por el tipo de fraude que interesa a este artículo es el siguiente:

En primer lugar, el emisor se encuentra obligado a ejecutar las órdenes de pago del usuario o de aquellas personas a quienes el usuario haya autorizado. De otra manera, incumple con su obligación contractual.

[39] Disponen los últimos tres incisos de la norma lo siguiente: "La Comisión para el Mercado Financiero, mediante norma de carácter general, establecerá estándares mínimos de seguridad, registro y autenticación. A través de la referida norma de carácter general, la Comisión determinará los supuestos de uso y transacciones en que resulte obligatorio por parte del emisor el uso de autenticación reforzada.
Para estos efectos, se entenderá por autenticación el procedimiento que permita al emisor comprobar la identidad del usuario o la validez de la utilización de un medio de pago, incluida la utilización de credenciales de seguridad personalizadas del usuario, y por autenticación reforzada, la utilización de al menos dos factores de autenticación, sea de conocimiento, posesión o inherencia, diferentes e independientes entre sí, para el acceso o utilización de los medios de pago, cuentas o sistemas similares que permitan efectuar pagos o transacciones electrónicas.
El emisor será responsable de los perjuicios que se deriven por el incumplimiento de los estándares mínimos de seguridad, registro y autenticación que determine la Comisión".

En segundo lugar, si tiene ocasión una orden de pago por alguien distinto del usuario, quien no ha sido autorizado por este último, debe distinguirse si el usuario ha dado o no noticia al emisor de que sus datos confidenciales necesarios para autorizar los pagos le han sido sustraídos. Si lo ha hecho, el emisor debe abstenerse de cursar cualquier pago e incumple, al menos, culposamente el contrato si lo hace.[40]

En tercer lugar, si el usuario aún no ha dado noticia, nuestra opinión es que debe distinguirse cómo ha llegado a ser el caso que el tercero accedió a la información confidencial del usuario necesaria para realizar la orden de pago.

Si el tercero ha obtenido la información del usuario o de personas por quienes este debe responder (art. 1679 Código Civil)[41] o, bien, de los equipos o dispositivos bajo el control del usuario, el riesgo es del usuario. Con todo, algún matiz es necesario. En primer lugar, por supuesto, la ley puede disponer las cosas de otra manera —la 20.009 lo hace—. Sin embargo, este es el escenario más allá de la ley 20.009. En ese escenario, lo que habrá que preguntarse, con cargo a regulación sectorial y las exigencias de la buena fe, es si el emisor debió haber actuado de alguna manera para evitar el resultado, así el ejemplo más claro se refiere al caso que las medidas de seguridad para la autenticación provistas por el emisor sean insuficientes.[42] Por otra parte, tratándose de los bancos, si no han informado a sus clientes acerca de los riesgos de phishing y el hecho que el banco nunca solicitará las claves, etc. En tercer lugar, según hemos visto, el emisor debe asumir el riesgo si, no obstante el hecho de que el tercero ha obtenido los datos confidenciales del usuario, las órdenes de pago arrojan patrones de conducta sospechosos que el emisor debió haber advertido.[43,44]

Si, en cambio, el tercero ha obtenido la información del emisor o de personas por quienes este debe responder, el riesgo es del emisor, en términos tales que deberá restituir lo pagado al usuario e indemnizar los daños causalmente conectados a su conducta. Lo anterior, por supuesto, bajo las reglas generales de derecho de contratos.

Conclusiones

El objeto de este trabajo consistió en explorar la distribución de los riesgos del phishing más allá de la ley 20.009, esto es, en aquellos casos en que la ley 20.009 no aplica. Nuestra hipótesis es que, en ese escenario, el riesgo es para quien está en mejores condiciones de controlarlo.

Consideramos que el recurso al depósito irregular de ciertas sentencias y un sector de la doctrina es incorrecto. Según nuestra opinión, de manera muy general, la relación entre el usuario y emisor se

[40] Desde luego, esto supone la existencia de un procedimiento de aviso y que el usuario lo cumpla. Sobre ese procedimiento de aviso se encuentra el punto "9.4. Pérdida, hurto, robo, falsificación o adulteración de la tarjeta" de la Circular N° 40 ya citada que se remite a la ley 20.009; "2.3.5 Pérdida, hurto, robo, falsificación o adulteración de la tarjeta" del Capítulo 8-41 RAN, y el punto 8 del título "III De los contratos de afiliación de entidades afiliadas; y entre el emisor y el operador" del Capítulo III.J.1 sobre "Emisión de Tarjetas de Pago" emitido por el Banco Central.

[41] Art. 1679: "En el hecho o culpa del deudor se comprende el hecho o culpa de las personas por quienes fuere responsable". Sobre la inteligencia de este artículo, ver De la Maza y Vidal, 2023, pp. 29-60.

[42] Así, por ejemplo, en De Lima con Banco del Estado de Chile (2019) se habla de "claves de seguridad" o "claves personales", redacción similar a la que se encuentra en la normativa sectorial, por ejemplo, los capítulos 1-7 y 8-41 RAN.

[43] En algunas ocasiones, la Corte ha señalado que el Banco tiene una obligación de monitorear y controlar la existencia de fraudes bancarios. Así, por ejemplo: Maluk con Banco de Chile (2020); Jaureguiberry con Banco Scotiabank de Chile (2020); Meza con Scotiabank Chile S.A. (2020) y Davagnino con Scotiabank Chile (2020).

[44] Si asumimos que la relación contractual que vincula al usuario y el emisor involucra un mandato, una de las formas que adopta el incumplimiento se manifiesta en el artículo 2149 del Código Civil, según el cual "El mandatario debe abstenerse de cumplir el mandato cuya ejecución sería manifiestamente perniciosa al mandante".

encuentra disciplinada por un contrato y es a través del régimen de los contratos, debidamente integrados por la buena fe (art. 1546 CC), que se debe resolver el problema. Siendo las cosas de esta manera, frente a un caso de phishing, la pregunta tendrá que administrarse desde la prestación del emisor. Si cumplió, no debe restituir al usuario lo pagado ni será responsable. Si incumplió, debe restituir y, según las normas generales sobre la materia, puede ser obligado a indemnizar los perjuicios.

Habrá incumplimiento del emisor si ejecuta indebidamente una orden de pago, y la orden de pago será indebidamente ejecutada si es que se realiza de una manera diversa a la debida (por ejemplo, si ingresándose datos incorrectos, igualmente se dio lugar a ella), si los datos son correctos, pero se obtuvieron del emisor o de personas por las que este responde o, si los datos son correctos, el tercero los obtuvo del usuario, pero la forma en que solicita la orden de pago resulta suficientemente irregular como para que el emisor pueda, razonablemente, constatarlo, en cuyo caso, debe abstenerse de ejecutarla.

En los demás casos, aunque se trate de un caso de phishing, el emisor cumple con su obligación, por lo mismo, nada debe.

Según nos parece, la aproximación contractual devela lo que el uso de la figura del depósito irregular mantenía oculto, y es que el riesgo debe asignarse a quien está en mejores condiciones de controlarlo. Esta tesis nos parece consistente con algunas decisiones de los tribunales superiores de justicia y con la normativa sectorial que está más allá de la ley 20.009.

Financiamiento

Este trabajo forma parte del proyecto de investigación "La protección del consumidor en la era digital" (PID2021-122985NB-I00), concedido por la Agencia Estatal de Investigación (España), del cual Iñigo de la Maza es coinvestigador.

Bibliografía

Alvear, Julio (2019). "El banco y nuestras cuentas corrientes". *Newsletter*, Noticias, 19 de junio de 2019.

Arancibia, María José (2017). *Tarjetas de Crédito. Responsabilidad de los bancos*. Santiago: DER Ediciones.

Arancibia, María José (2021). "Responsabilidad civil por fraude bancario. El nuevo régimen aplicable a las operaciones electrónicas". En Lepin, Cristian y Stitchkin, Nicolás (dirs.). *Estatutos especiales de responsabilidad civil*. Valencia: Tirant lo Blanch.

Campos, Sebastián (2021). "Función suplementaria de la buena fe contractual y deberes derivados. Un análisis a la luz del moderno derecho de contratos". *Revista Chilena de Derecho Privado*, N° 37, pp. 105-159.

Campos, Sebastián; Munita, Renzo y Pereira, Esteban (2022). "Fundamentación normativa de los deberes derivados de la buena fe contractual. Entre el individualismo desinteresado y el altruismo moderado". *Revista de Derecho Privado*, N° 43, 187-2017.

Cordero, Luis y Contardo, Juan Ignacio (2020). "Regulación de los riesgos del fraude bancario: algunas interrogantes que deja la nueva Ley N° 21.234". *El Mercurio Legal*, 26 de agosto de 2020.

Corral, Hernán (2019). "Fungibilidad del dinero y riesgo de fraude bancario". *El Mercurio Legal*, 12 de julio de 2019.

De la Maza, Iñigo y Loayza, Boris. "Phishing y distribución del riesgo". Artículo envido para publicación.

De la Maza, Iñigo y Vidal, Álvaro (2023). "La exterioridad del caso fortuito y la esfera de control". *Revista de Derecho Civil*, vol. X, núm. 4 (julio-septiembre, 2023), pp. 29-60.

Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE.

Fernández, Felipe y Labra, Ignacio (2023). "Contrato de mutuo o préstamo de consumo". En Munita, Renzo (dir.). *Contratos. Parte especial*. Valencia: Tirant lo Blanch.

Guzmán Brito, Alejandro (2002). "La buena fe en el Código Civil de Chile". *Revista Chilena de Derecho*, Vol. 29 N° 1, pp. 11-23.

Guzmán Brito, Alejandro (2014). "El depósito irregular en el derecho chileno". *Revista Chilena de Derecho Privado*, N° 23, pp. 87-137.

Haley, David (2015). "What is a Commercially Reasonable Security Procedure Under Article 4a of the Uniform Commercial Code?", en *Fidelity Law Journal,* vol XXI.

Mayer, Laura y Oliver, Guillermo (2020). "El delito de fraude informático: Concepto y delimitación", en *Revista Chilena de Derecho y Tecnología*, vol. 9 núm. 1, pp. 151-184.

Momberg, Rodrigo (2013). "Artículo 1° N° 1". En De la Maza, Iñigo y Pizarro, Carlos (dirs). *La Protección de los Derechos de los Consumidores. Comentarios a la Ley de Protección a los Derechos de los Consumidores*. Santiago: Thomson Reuters.

Munita, Renzo (2023). "Bancos, clientes y fraudes vía actos de phishing o de pharming". En Díaz, Karenn y Guthrie, Hans (dirs.). *Estudios de Derecho del Consumidor*. Valencia: Tirant lo Blanch.

Munita, Renzo y Aedo, Cristian (2020). "Responsabilidad civil de los bancos por fraudes informáticos a la luz de la ley de protección de los consumidores", en *Actualidad jurídica*, N° 42, julio 2020, pp. 73-106.

Oxman, Nicolás (2013). "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*, XLI, pp. 211-262.

Rabin, Robert (1999). "Enabling Torts", en *DePaul Law Review*, vol. 49, 1999, pp. 435-454.

Reglamento (UE) nº 1093/2010 y se deroga la Directiva 2007/64/CE.

Rodríguez, Javier (2019). "Depósito irregular y restitución de fondos sustraídos en fraude bancario. Corte Suprema, 13 de marzo de 2019, Rol N.° 29.635-2018". *Revista Chilena de Derecho Privado*, N° 33, pp. 193-204.

Tomarelli, Feliciano (2020). "Responsabilidad civil por fraude bancario". En Elorriaga, Fabián (ed.). *Estudios de Derecho Civil XV*. Santiago: Thomson Reuters.

Turner, Paul (1994). "The UCC Drafting Process and Six Questions about Article 4A: Is There a Need for Revisions to the Uniform Funds Transfers Law", en *Loyola of Los Angeles Law Review,* vol. 28.

Sentencias citadas

Alviña con Banco de Chile (2019): Corte Suprema, 14 de agosto de 2019, Rol N° 7155-2019.

Arriaza Aguilera con Banco Scotiabank (2021): Corte de Apelaciones de San Miguel, 13 de diciembre de 2021, Rol N° 132-2021.

Ayala con Banco Scotiabank Chile (2021): Corte Suprema, 4 de abril de 2021, Rol N° 131079-2020.

Banco del Estado de Chile con José Luis Rocco Tachi Red de Suministros Eléctricos EIRL (2023): Corte de Apelaciones de Santiago, 8 de mayo de 2023, Rol N° 1508-2021.

Cabrera con Banco del Estado de Chile (2020): Corte de Apelaciones de Temuco, 25 de marzo de 2020, Rol N° 5895-2019.

Cañas con Banco Scotiabank Chile (2020): Corte de Apelaciones de Santiago, 16 de junio de 2020, Rol N° 25798-2020.

Claudio Luna Zurita con Banco de Chile (2023): Corte de Apelaciones de Santiago, 6 de enero de 2023, Rol N° 252-2020.

Comercial Piña Espina y Cía. Ltda. con Banco de Chile (2020): Corte Suprema, 10 de junio de 2020, Rol N° 24817-2020.

Comercializadora y Distribuidora Mauricio Lainez Rojas E.I.R.L. con Banco de Chile (2020): Corte de Apelaciones de Iquique, 31 de agosto de 2020, Rol N° 549-2020.

Davagnino con Scotiabank Chile (2020): Corte de Apelaciones de Valdivia, 22 de octubre de 2020, Rol N° 2805-2020.

De Lima con Banco del Estado de Chile (2019): Corte de Apelaciones de Valparaíso, 8 de agosto de 2019, Rol N° 10271-2019.

Distribuidora de Materiales de Construcción S.A.C. con Banco de Chile (2023): Corte de Apelaciones de Santiago, 26 de mayo de 2023, Rol N° 80690-2022.

Gutiérrez con Scotiabank Chile S.A. (2021): Corte Suprema, 20 de enero de 2021, Rol N° 131051-2020.

Irma Simunovic Fadic con Banco Santander Chile S.A. (2023): Corte de Apelaciones de Santiago, 8 de junio de 2023, Rol N° 1756-2021.

Luz Jaureguiberry Labbé con Banco Scotiabank de Chile (2020): Corte de Apelaciones de Concepción, 26 de junio de 2020, Rol N° 8120-2020.

Maluk con Banco de Chile (2020): Corte de Apelaciones de Valparaíso, 17 de febrero de 2020, Rol N° 40789-2019.

Meza con Scotiabank Chile S.A. (2020): Corte de Apelaciones de Rancagua, 28 de julio de 2020, Rol N° 2175-2020.

Millar con Banco Scotiabank Chile S.A. (2020): Corte de Apelaciones de Temuco, 29 de septiembre de 2020, Rol N° 2058-2020.

Muñoz con Banco del Estado de Chile (2020): Corte de Apelaciones de Valparaíso, 31 de enero de 2020, Rol N° 40222-2019.

Palma con Banco de Chile (2019): Corte de Apelaciones de Iquique, 30 de diciembre de 2019, Rol N° 1004-2019.

Péndola con Banco Scotiabank (2023): Corte Suprema, 27 de junio de 2023, Rol N° 59554-2020.

Ramírez Cardemil con Banco de Chile (2019): Corte de Apelaciones de Concepción, 6 de agosto de 2019, Rol N° 12685-2019.

Requena con Banco Scotiabank (2020): Corte Suprema, 28 de diciembre de 2020, Rol N° 50564-2020.

Ruiz con Banco de Chile (2020): Corte de Apelaciones de Santiago, 10 de agosto de 2020, Rol N° 34308-2019.

Troncoso con Banco Scotiabank Chile (2021): Corte Suprema, 23 de marzo de 2021, Rol N° 139905-2020.

Valdés con Sardon (2020): Corte de Apelaciones de Iquique, 23 de abril de 2020, Rol N° 177-2020.

Zúñiga con Itaú Corpbanca S.A. (2020): Corte Suprema, 17 de noviembre de 2020, Rol N° 131150-2020.