DOCTRINA PRÁCTICA

La responsabilidad civil de los bancos por el riesgo de *phishing*

José Campos Bermúdez*

Universidad Nacional Mayor de San Marcos

SUMARIO

RESUMEN

Se reflexiona sobre los siguientes puntos: ¿quién asume el riesgo en una contratación financiera por medio de uso de la tecnología?, ¿cómo se verifica el cumplimiento de los mecanismos de seguridad de los bancos?, ¿si la modalidad del *phishing* es un patrón de fraude reiterativo, el banco tiene o no la obligación legal de realizar un análisis sistemático y tomar las medidas de seguridad pertinentes?, entre otros puntos.

Palabras clave: Idoneidad / Riesgos típicos de operaciones / Cláusulas de adhesión

Recibido: 22-08-18
Aprobado: 03-10-18
Publicado en línea: 02-11-18

ABSTRACT

It reflects on the following points: who assumes the risk in a financial contracting through the use of technology? How is the compliance of the security mechanisms of the banks verified? If the phishing modality is a standard of reiterative fraud, the bank does or does not have the legal obligation to carry out a systematic analysis and take the relevant security measures, among other points.

Keywords: *Suitability / Typical operational risks / Accession clauses*

Title: *The liability of banks for the risk of phishing*

Author: *José Campos Bermúdez*

* Abogado por la Universidad Nacional Mayor de San Marcos. Magíster en Derecho Civil por la Pontificia Universidad Católica del Perú. Socio del Estudio Campos, Herbozo & Toribio Abogados.

1. Introducción

El *phishing* en uno de los fraudes por Internet más complejos, masivos y peligrosos que se presentan en la industria bancaria. El término *phishing* deriva del inglés *fishing* ('pesca') y se emplea porque en este tipo de fraudes se busca que la víctima "muerda el anzuelo". Esta modalidad de fraude cibernético, que consiste en el hurto de la identidad digital para obtener un lucro indebido, se verifica a través del envío de un correo electrónico al cliente bancario con la indicación —suplantando la cuenta e imagen oficial de una entidad bancaria— de que se requiere la actualización de su datos debido a motivos de seguridad, que la cuenta será desactivada si no lo hace, o que ha sido favorecido con un premio, siendo necesario para ello que digite su tarjeta, clave y contraseña en el *link* que contiene el mensaje.

De esta forma, y engañado por la apariencia legítima del correo emisor y la página web clon a la oficial que se abre una vez hecho *click* en el *link*, la víctima digita sus datos, clave y contraseña, que son enviados al impostor, sin suponer que con ellos este podrá concretar el fraude bancario. Tal fraude se ejecutará empleando el Internet a través de dos formas: la primera de ellas mediante operaciones a través del canal de atención del banco denominado "banca por Internet", transfiriendo los fondos de la cuenta de la víctima hacia las cuentas de otras personas denominadas muleros (que forman parte de la cadena delictiva); y la segunda mediante compras o pagos por Internet, con cargo a las tarjetas de débito o crédito de la víctima.

Todas estas operaciones, evidentemente, no son reconocidas como propias por las víctimas, quienes, al conocerde ellas, denuncian el fraude antebanco, que procede al bloqueo de las tarjetas. Dependiendo del procedimiento de atención del banco, algunas veces las víctimas se enteran cuando les llegan sus estados de cuenta, otras cuando consultan sus saldos, y otras cuando el mismo banco las advierte de las operaciones sospechosas realizadas.

El problema es que, para cuando se enteran de las operaciones fraudulentas, es tarde porque los fondos ya fueron retirados de sus cuentas de ahorros o ya se dispuso de las líneas asignadas en las tarjetas de crédito. Como ya lo anotamos, el banco procede al bloqueo de las tarjetas para evitar futuros fraudes, pero para cuando eso ocurre las pérdidas de las víctimas ya se produjeron, es decir, el daño patrimonial se verificó.

De acuerdo con la 19.º Encuesta Global de Seguridad de la Información[1] (Ernst & Young), el *phishing* se encuentra dentro de las amenazas en crecimiento más importantes, ya que pasó de 39 % en el 2014 y 44 % en el 2015 a 51 % en el 2016. Esta modalidad de fraude se ha incrementado mucho en

1 Lampadia, "Fortaleciendo las capacidades de seguridad cibernética". Recuperado de <https://bit.ly/2H8WBZm>.

Número 52 • Octubre 2018 • pp. 277-302
ISSN 2313-4828 (impresa) • ISSN 2415-2277 (en línea)

América Latina y el Perú, a tal punto que se sostiene que su práctica está un 20 % por encima que en el resto del mundo[2]. Tal es la magnitud de este problema, que se reconoce que el 98.5 % de los riesgos bancarios en América Latina son informáticos, que antes el riesgo era físico (robos en las oficinas) y ahora es digital, siendo el *phishing* uno de los más importantes[3]. Y es que, como lo ha reconocido un gerente de seguridad integral de un banco[4], los fraudes vienen migrando de presenciales a ser no presenciales, lo cual se explica por los nuevos riesgos que van apareciendo con el desarrollo tecnológico. Lo expuesto demuestra que la situación es muy grave[5] [6].

La importancia del tratamiento jurídico de este problema proviene también del hecho de que —como lo informa el Indecopi—, de los 59 217 reclamos recibidos durante el periodo de abril del 2016 a marzo del 2017, el 53,35 % corresponde a la actividad bancaria y financiara, y gran parte de ellos se presentan con las tarjetas de crédito y, asociados a ella, una serie de problemas por consumos fraudulentos[7].

2. La banca por Internet

Como vemos, el desarrollo tecnológico y los nuevos productos y servicios que operan en el ciberespacio han traído consigo nuevos riesgos. Los bancos vienen reforzando sus medidas de seguridad para evitarlos, pero es claro que estos se siguen presentando y es importante establecer que lo hacen en el desarrollo de su actividad, en particular en la plataforma de lo que se ha venido en denominar banca por Internet, devenida hoy en la nueva forma de comunicación entre el banco y sus clientes, que permite a estos, a través de una computadora o un *smartphone*, realizar operaciones de manera virtual cuando lo necesiten.

Desde hace varios años los bancos empezaron a ofrecer a sus clientes la posibilidad de llevar a cabo sus operaciones a través de su plataforma de servicios de Internet, y vienen fomentando la migración de sus clientes hacia estos medios. Ello en razón a que se considera que estos son más baratos que la sucursal y mejoran la eficiencia[8].

2 El Comercio, "'Phishing' y 'bots': las amenazas al comercio en Latinoamérica". Recuperado de <https://bit.ly/2O1r1ow>.

3 Agencia Efe, "El 98,5 de los riesgos bancarios en América Latina son informáticos". Recuperado de <https://bit.ly/2OwAfZE>.

4 Perú 21, "Aumentan ciberataques en el Perú: ¿Por qué pensamos que nunca nos pasará a nosotros?". Recuperado de <https://bit.ly/2P3Yonc>.

5 RPP, "Cerca de 700 personas al mes son víctimas de fraude bancario". Recuperado de <https://bit.ly/2LN0KWe>.

6 La República, "Vacían cuenta de ahorros clonando página web de entidad bancaria". Recuperado de <https://bit.ly/2QrMQua>.

7 Gestión, "Indecopi: 45 de cada 100 reclamos son contra entidades financieras", Recuperado de <https://bit.ly/2spFoWQ>.

8 Gestión, BCP, "Nuestra principal competencia no es otro banco, sino el dinero en efectivo". Recuperado de <https://bit.ly/2NloksF>. El gerente general del BCP Walter Bayly reconoció en esta entrevista que "es bien caro atender en la ventanilla, por eso hemos hecho

Es claro que la banca por Internet reduce los costos de los clientes, quienes no gastan en transporte para acudir a las oficinas del banco, ahorrando tiempo y tienen una mejor disponibilidad de su horario, además de reducir el riesgo de robos al no tener que transportar altas cantidades de dinero.

No obstante estos beneficios, nos preguntamos: ¿invierten lo suficiente los bancos en las medidas de seguridad de sus sistemas de seguridad informático?[9], ¿informan suficientemente a sus clientes de los riesgos que genera el uso de la plataforma de banca por Internet? Y frente a la ocurrencia frecuente de estos fraudes bancarios, nos continuamos interrogando: ¿quién debe asumir sus consecuencias?, es decir, ¿quién debe asumir la pérdida del dinero apropiado por los delincuentes? Los bancos culpan a sus clientes de no tomar las medidas de seguridad y proporcionar sus datos a terceros y los clientes responsabilizan a los bancos de que sus sistemas de seguridad e información no son los adecuados, que dichos daños se dan con ocasión de la prestación del servicio bancario, por lo que son los bancos los que deben asumir los riesgos de su actividad.

3. La "solución" del Indecopi

En las denuncias que se presentan ante el Indecopi, los consumidores alegan que el banco no adoptó las medidas de seguridad consistentes en (i) la verificación del patrón de uso de las operaciones realizadas con sus tarjetas de crédito y débito; (ii) alertas de operaciones inusuales; y (iii) permitir que se realicen las operaciones no reconocidas.

Frente a tales imputaciones, los bancos replican que las medidas de seguridad aplicadas a las tarjetas de débito o crédito del consumidor se materializan con el bloqueo preventivo de ellas luego de efectuado el reporte de las operaciones no reconocidas, para evitar que dichas tarjetas sigan utilizándose. Señalan, además, que las alertas o monitoreo de transacciones se realizaba tomando como referencia la línea de crédito del cliente. Asimismo, se amparan en los contratos de "Términos y condiciones generales para el uso de las tarjetas" suscritos por el cliente,

un esfuerzo muy grande de derivar nuestros clientes hacia canales alternativos, internet, agentes […]". Y es que, en efecto, si revisamos la publicidad no solo del BCP, sino también de otros bancos, podemos observar que estos constantemente nos empujan a utilizar la plataforma del Internet para realizar operaciones bancarias. La razón ya la dio el mencionado representante legal del banco: ahorrar costos, es decir, ganar más dinero, que la actividad bancaria sea más rentable.

9 Si revisamos la publicidad televisiva del BCP, por ejemplo, en los últimos años, vemos una alta inversión en la promoción de sus productos tales como cuentas premio, (árbol, microondas, ahorrar para ganar, etc.), en tus planes *contigo BCP*, *Ir al banco sin ir al banco* ("'¿lobo que estás haciendo?', 'banca por Internet, Manu'", etc.), pero no hemos encontrado ni la más mínima publicidad alertando los peligros de la plataforma de Internet. Existe una alarmante y reveladora desproporción entre la publicidad sobre la promoción del uso del Internet y la publicidad sobre las medidas de seguridad que requiere el uso de esa plataforma de servicio.

Número 52 • Octubre 2018 • pp. 277-302
ISSN 2313-4828 (impresa) • ISSN 2415-2277 (en línea)

que establece la responsabilidad de este respecto a la utilización de su tarjeta de débito y claves secretas, siéndole imputable cualquier operación de verificarse la presencia de los elementos indicados, ya que ellas se reputan como realizadas por el cliente, toda vez que es la única persona que debe mantener bajo su cuidado la información de su tarjeta y de las claves secretas, lo cual excluye de cualquier tipo de responsabilidad al banco.

Para el Indecopi, el parámetro de idoneidad del banco en este tipo de operaciones vía Internet es la verificación de los mecanismos de seguridad implementados por los bancos, pero el problema es que, para tal verificación representativa de la "idoneidad" del banco, se identifica, erróneamente a nuestro juicio, la seguridad en la operación con la sola digitación de los datos y claves. De tal modo, verificados que estos fueron digitados, el Indecopi considera válida la operación.

Esta perspectiva de seguridad en la operación, como desarrollaremos más adelante, es evidentemente restrictiva e incorrecta, ya que no reconoce toda la realidad de la misma; es decir, el estándar de cumplimiento de seguridad de los bancos a la que irreflexivamente se adhiere el Indecopi no es compatible con la realidad completa de la operación y los riesgos inherentes a ella. Así las cosas, las resoluciones del Indecopi no solucionan el problema, sino que más bien lo agrava dejando en peor condición a la víctima.

En efecto, tiene establecido el Indecopi que, para validar las operaciones por Internet no reconocidas por los consumidores, las entidades financieras deberán presentar la documentación que acredite que las transacciones se realizaron con el empleo de los datos de la tarjeta del cliente y el empleo de las claves secretas[10]. De este modo, si el banco prueba que las operaciones se efectuaron ingresando las claves y contraseñas, las denuncias de los clientes son declaradas infundadas.

Ahora bien, la carga de la prueba de la realización de las operaciones no reconocidas la tiene el banco. Así lo ha expresado el Indecopi[11], y ello porque, como resulta lógico, la comprobación de un hecho negativo —como la no realización de transferencias de dinero— no es factible para el denunciante. Por tal razón, es el banco quien debe probar que dicho hecho negado sí se produjo, y para ello debe presentar la documentación que acredite que las transacciones se realizaron con el empleo de los datos de la tarjeta del cliente y de las claves secretas, que permiten validar las operaciones.

10 Resolución N.º 762-2010/SC2, del 19 de abril de 2010, en el procedimiento seguido por la señora María Esther Cárdenas Valencia en contra de Scotiabank Perú SAA; Resolución N.º 2684-2010/SC2, del 29 de noviembre del 2010, en el procedimiento seguido por el señor Christian Burgos del Campo.

11 Resolución N.º 270-2008/TDC-INDECOPI, de fecha 13 de febrero del 2008, de la Sala Especializada en Protección al Consumidor, antes Sala de Defensa de la Competencia N.º 2.

Este es el estado de la cuestión, los tribunales del Indecopi no encuentran responsabilidad en los bancos por este tipo de fraudes, porque considera suficiente que estos acrediten, con los reportes de sus aplicativos Homebanking y Log Ace Server, que las operaciones se efectuaron correctamente, empleando los datos de la tarjeta y claves secretas.

Como si el problema de seguridad tuviera que ver solo con las computadoras del consumidor, la posición del Indecopi, en una visión sesgada y parcial del conjunto de la realidad, es que no se puede responsabilizar al banco por no tomar las medidas de seguridad para proteger la seguridad de tales computadoras, ya que dicha tarea es de responsabilidad de los propios consumidores, quienes tienen que velar además por la seguridad de las conexiones que establecen para ingresar a la página web del banco.

Respecto de su obligación de monitoreo de las operaciones, considera el Indecopi que la finalidad del sistema de monitoreo no es que el cliente autorice una operación ya ejecutada, en la medida que no se pueden anticipar operaciones, sino que, una vez generada una alerta, este procede al bloqueo de la tarjeta para evitar que se pudieran realizar más operaciones fraudulentas.

Con la misma visión parcial del problema, considera además el Indecopi que el fraude en todo caso es obra de un tercero ajeno al banco, quien, aprovechándose de un descuido del cliente, logra acceder a su información financiera, hecho en el cual el banco no participa, por lo que resulta erróneo imputarle una conducta ajena realizada fuera de su esfera de control y seguridad.

Ratificando el incorrecto reparto de los riesgos presentes en la operación realizado por el banco, el Indecopi considera que su control compete al consumidor, quien,, sobre la base de la información existente en el mercado, comprende que existe un riesgo en el empleo de tarjetas de crédito y débito, de modo que está en aptitud de conocer que existe la posibilidad de que, si no tiene especial cuidado, terceras personas pueden acceder a su tarjeta y realizar consumos con ella.

Esta situación es sumamente injusta porque esa verdad formal que abraza el Indecopi no se corresponde con la verdad real. En efecto, no es verdad que las operaciones las hayan efectuado los consumidores, ellos reclaman precisamente porque las desconocen, de modo que si el Indecopi asume la posición de los bancos, lo que está haciendo en buena cuenta es considerar mentirosos a los múltiples clientes que reclaman o, en el mejor de los casos negligentes, responsabilizándolos de no tomar sus medidas de precaución para evitar que estos daños se concreten. Frente a ello, nos preguntamos: ¿quién desarrolla la actividad?, ¿quién se vale del Internet para prestar sus servicios?, ¿quién debe gestionar los riesgos típicos de su actividad profesional? ¿No es acaso el *phishing* un riesgo de la actividad bancaria?

Número 52 • Octubre 2018 • pp. 277-302
ISSN 2313-4828 (impresa) • ISSN 2415-2277 (en línea)

Como se soslaya en las resoluciones de Indecopi, los bancos tienen la obligación, impuesta por la ley, de identificar patrones de fraude mediante el análisis sistemático de la información histórica de las operaciones, los que deberán incorporarse al sistema de monitoreo de las mismas, para así tomar las medidas correspondientes para evitar que su sistema informático sea fácilmente vulnerable. Al parecer, los bancos lo están haciendo, pero no en el nivel deseado que impida los riesgos de fraudes y esto se debe a que, como lo reconoce uno de sus más connotado representantes, "hemos estado en los últimos años preocupados en capturar el crecimiento más que necesariamente en ser los más eficientes y creo que tenemos una tarea pendiente ahí"[12].

Es decir, la eficiencia pasó a un segundo plano, los clientes son una tarea pendiente. Claro, esto explica la nota de *El Comercio* denominada "Las utilidades de los bancos crecieron 35 % hasta setiembre"[13], es decir, los bancos han ganado más que el promedio del país, y en el caso del "BCP mejoraron un 43.5 %". Nos parece bien que el banco haya ganado mucho más que el resto, pero los casos de pérdidas de consumidores por *phishing* son una clara evidencia de que hay pasivos que el banco no ha asumido, que hay pérdidas provocadas por la indebida gestión de sus riesgos operacionales que no ha asumido, y que, bajo las reglas de la responsabilidad civil, la consideración de la profesionalidad de su actividad, la tutela del consumidor al sistema experto que representa y la justica, le correspondería hacerlo..

IMPORTANTE

[…] desarrollo tecnológico y los nuevos productos y servicios que operan en el ciberespacio han traído consigo nuevos riesgos. Los bancos vienen reforzando sus medidas de seguridad para evitarlos, pero es claro que estos se siguen presentando y es importante establecer que lo hacen en el desarrollo de su actividad, en particular en la plataforma de lo que se ha venido en denominar banca por Internet, devenida hoy en la nueva forma de comunicación entre el banco y sus clientes, que permite a estos, a través de una computadora o un *smartphone*, realizar operaciones de manera virtual cuando lo necesiten.

No conocemos de reclamos contra los bancos que se hallan judicializado, pero sí de muchas denuncias presentadas ante el Indecopi, entidad que en la mayoría de los casos se pronuncia a favor de los bancos, considerando erróneamente y sin tener en cuenta que el *phishing* es un riesgo típico operacional de su actividad, que fue la falta de cuidado del cliente la causa de que se hayan producido estos daños, que el riesgo lo asume

12 Gestión, BCP, "Nuestra principal competencia no es otro banco, sino el dinero en efectivo", art. cit.

13 El Comercio, "Las utilidades de los bancos crecieron 35% hasta setiembre". Recuperado de <https://bit.ly/2RjxadM>.

él según lo "pactado" en el contrato de adhesión que firmó con el banco.

Solo en los casos en que los bancos no han podido demostrar por error en el registro de sus sistemas informáticos que las operaciones no se realizaron con las claves y contraseñas de los consumidores, o en los que los retiros se produjeron luego del aviso de bloqueo efectuado por los consumidores, el Indecopi ha fallado a favor de estos. Hemos encontrado sí que algunos de estos casos fueron judicializados por los bancos, buscando la nulidad de las resoluciones del Indecopi. Así, mediante sentencia de fecha 24 de abril del 2014, emitida por la Octava Sala Especializada en lo contencioso administrativo con subespecialidad en temas de mercado (Exp. N.° 669-2008), se declaró infundada la demanda presentada por el Scotiabank Perú SAA, y se sostuvo lo siguiente:

> […] *SÉTIMO*: Ahora bien, la reducción del riesgo de uso fraudulento de la tarjeta de crédito o de débito, es necesaria para la consolidación del sistema financiero. Para lo cual resulta indispensable que se den medidas de seguridad eficientes y eficaces que vayan de acuerdo con la realidad y los cambios tecnológicos, para que cumplan con los dos objetivos principales que son por un lado la reducción de usos no autorizados o fraudulentos de las tarjetas en mención y, por el otro lado, la protección al consumidor.
>
> Así, a fin de que los usos no autorizados o fraudulentos de las tarjetas de crédito y/o débito descienda, los bancos y entidades financieras deben implementar sistemas preventivos de monitoreo de transacciones y procedimientos complementarios, que permitan detectar razonablemente aquellas que pueden corresponder a patrones de fraude; ello con el objeto de evitar actividades potencialmente indebidas o someterlas a mayor escrutinio y verificaciones adicionales. Lo que se busca con ello primordialmente es que, al no tener el usuario cómo detectar sus consumos en tiempo real, las entidades financieras sean minuciosas al efectuar la autorización de las transacciones realizadas por sus clientes […].
>
> *NOVENO:* Tanto más cuando, los transgresores dedicados a estas actividades (clonación de tarjetas de crédito o débito, toma los datos en los POS, dispositivos inalámbricos que cuentan con un sistema informático para la transferencia de datos a un procesador, que se almacenan) se tornan cada vez más sofisticados, de forma tal que se crean nuevas formas de acceder a los datos de los usuarios de las mismas, incluyendo su clave secreta.
>
> En tal sentido, no resultan atendibles los argumentos señalados por la demandante, en tanto que se aprecia que la entidad bancaria no ha actuado conforme a su deber de prestar un servicio idóneo; tanto más si lo que se espera de una entidad de tal naturaleza es la conservación del dinero de manera que no se vea afectado o mermado por efectos de un robo o apropiación ilícita, por el ejercicio de actividades delictivas; que en este caso están en la posición de poder detectar, más aún si en el sistema figuran los retiros, resultando inusual que el titular retire diferentes montos en momentos diferentes el mismo día, cuando lo puede hacer en una sola ocasión, dado que —como ya se ha acreditado— no se ha excedido el monto máximo de retiro por cada ocasión y/o en el día.
>
> Así, se espera de la entidad bancaria realicen todos los esfuerzos a efectos de garantizar que las operaciones sean realizadas por el cliente, y no por terceros. Siendo su responsabilidad prever las posibilidades de fraude así como instalar los mecanismos prácticos

Número 52 • Octubre 2018 • pp. 277-302
ISSN 2313-4828 (impresa) • ISSN 2415-2277 (en línea)

> y elementales para detectarlos, además de los electrónicos […].

Como vemos, el Poder Judicial en este caso confirmó la decisión del Indecopi, pero este era uno en el que el banco solo presentó copia de las *winchas* auditoras que no podían demostrar que las operaciones se realizaron con las claves y contraseñas del consumidor. Debido a este defecto de probanza del banco, el Indecopi falló en su contra y fue más sencillo al Poder Judicial confirmar tal decisión. Sin embargo, lo que pasó aquí no es lo más común. En la gran mayoría de los casos los bancos, sí pueden satisfacer tal probanza y entonces los consumidores no reciben la tutela que esperaban, y desalentados tampoco judicializarán estas decisiones adversas.

4. La recortada "realidad" que emana del contrato de adhesión y su corrección por la buena fe

En los casos en que se presentan los daños al consumidor por estas operaciones fraudulentas de *phishing*, los bancos suelen invocar en su defensa a las condiciones generales que habrían "pactado" con sus clientes. En efecto, los bancos se amparan en el carácter "indudable" cual máxima de la ciencia de que las operaciones efectuadas con los datos y claves las realizó su cliente, y que ese carácter se habría "pactado" en las referidas condiciones generales. Al respecto, reparamos que en realidad exista un "pacto" o "acuerdo" que provenga de la negociación de las partes, porque el contrato bancario es efectuado bajo la modalidad de adhesión, en el que el pacto es solo una ficción jurídica y en el que el predisponente no puede excluirse de la responsabilidad.

En efecto, en estos contratos de adhesión representativos del sistema experto con que se presenta el servicio bancario frente al consumidor, no existe una verdadera "común intención de las partes", de modo que, como afirma el profesor Juan Espinoza, indagar sobre ella sería "ciencia ficción"[14]. Además, como anota Schiesaro, la disciplina de las condiciones generales del contrato con que se intentaba proteger al contratante adherente frente al riesgo de abuso más bien lo legitimaba favoreciendo al predisponente[15].

Y es que la experiencia ha demostrado que estos predisponen los reglamentos asumiendo algunas veces desfasada y otras descaradamente, y con la venia o silencio del legislador y algunos jueces también desfasados, que dichos reglamentos serán ley entre las partes, que tendrán sin indulgencia alguna, carácter vinculante para el consumidor, perdiéndose de vista que, en realidad, esa vinculación es ilusoria, ciencia ficción.

Esa indebida distribución de riesgos, que llevaría a asumir al consumidor

14 Espinoza Espinoza, Juan, *Acto Jurídico Negocial. Análisis doctrinario, legislativo y jurisprudencial*, Lima: Gaceta Jurídica, 2008, p. 247.

15 Schiesaro, Diego Angelo, "El contrato asimétrico", *Actualidad Civil*, n.° 22, Lima: 2016, p. 111.

el costo de los fraudes, es precisamente un elemento que engendra un desequilibrio supino en la relación, un abuso de derecho que el sistema jurídico en general y el sistema de protección al consumidor en particular (art. 47.b, art. 48.c) proscriben. Constituye, de hecho, dicha cláusula una cláusula abusiva (art. 49) que no debe ser aplicada por los órganos que administran justicia.

Dicho indebido traslado de riesgos en contra del consumidor, esa exclusión de responsabilidad del banco y esa interpretación *pro proferentem*, vedados como hemos dicho por nuestro sistema legal, es lo que respalda la posición de los bancos.

Nuestro ordenamiento civil también es claro sobre este tema. El artículo 1398 del Código Civil establece: "En los contratos celebrados por adhesión y en las cláusulas generales de contratación no aprobadas administrativamente, no son válidas las estipulaciones que establezcan, en favor de quien las ha redactado, exoneraciones o limitaciones de responsabilidad […]". En ese sentido, las cláusulas que invocan los bancos no pueden ser oponibles porque no son válidas. Y no podría ser de otro modo, dado que por la propia naturaleza de la actividad financiera que constituye un "sistema experto"[16], el que debe asumir la responsabilidad por los riesgos y daños generados es el propio banco, quien tiene la obligación de gestionarlos en el desarrollo de su actividad.

Cabe añadir que uno de los propósitos del Código de Consumo contemplado en su artículo II es la corrección de conductas y prácticas que afecten los legítimos intereses de los consumidores. Esta función correctora alude a un estado de anormalidad que puede presentarse en una relación de consumo por conductas (incumplimientos) o prácticas (contratos de adhesión, abuso de posición de dominio, exclusión de responsabilidad, indebido reparto de riesgos, etc.) que afectan los intereses legítimos de los consumidores.

La confianza no solo es un elemento del sistema experto, sino además una expresión del principio de la buena fe. Es esta la que debe guiar la conducta de las partes, y para ello se deben analizar las circunstancias relevantes del caso, como la información brindada, las características de la contratación y otros elementos de la operación, de lo que ya hemos dado cuenta antes. Como resulta claro, la confianza no puede dejar de estar presente en la relación con una entidad financiera, por ser consustancial a ella.

Dado que el consumidor que suscribe el contrato con el banco solo puede aceptarlas o rechazarlas en su conjunto, sin poner reparo a los alcances de alguna de ellas, es necesario evitar el abuso del predisponente, reequilibrándolo con apoyo de este instrumento de justicia contractual como es la buena fe.

16 Campos Bermúdez, José A., *La responsabilidad civil de los bancos en compras financiadas en planos de inmuebles y en operaciones por Internet*, Lima: Instituto Pacífico, 2018, p. 65 y ss.

Número 52 • Octubre 2018 • pp. 277-302
ISSN 2313-4828 (impresa) • ISSN 2415-2277 (en línea)

5. Los *phisher* no son los terceros en que se ampara el banco para responsabilizar al consumidor

Cuando en su defensa los bancos invocan como conducta causante de los daños el que el cliente facilitara a los terceros sus claves secretas que debió mantener en custodia, expresa en realidad una falacia y demuestra lo desfasado de sus argumentos frente a la modalidad de fraude electrónico tratado en este trabajo, lo cual es muy preocupante y revela porqué este tipo de fraudes son muy comunes en la actividad bancaria.

Decimos eso porque, primero, en rigor, esa "entrega" no se produce. En efecto, el cliente no ha entregado sus claves a terceros. No ha habido una conducta positiva de entrega de una persona (el consumidor) a otra (los estafadores), lo que ha habido es simplemente una digitación de las claves en el contexto de una petición efectuada por quien se supone es el banco. La digitación de las claves y contraseñas no se realizan con el propósito de entregarlas a un tercero, sino simplemente para atender un requerimiento que se supone legítimo del banco.

No estamos ante el caso en el cual el cliente entrega de las claves a un familiar o un amigo, quienes sí tendrían la condición de terceros y estos realizarán consumos u operaciones. Para las referidas condiciones generales, el tercero es esa persona que recibe la clave del titular para hacer operaciones con cargo a su cuenta. Lo acontecido en el caso de *phishing,* sin embargo, es distinto.

Esta errónea concepción de tercero que asume el banco y el Indecopi es muy importante de destacar, porque nos permite reconocer los contornos de la verdadera realidad de los casos de estudio y cuestionar la recortada "realidad" que ha sido asumida por las indicadas entidades, aquella que privilegia la formalidad que el banco acostumbra proyectar, es decir, de que el cliente "pactó" o que "entregó a un tercero", amparándose en el contrato que predispuso.

En segundo lugar, es una falacia, porque las reales circunstancias de una relación de consumo al amparo del principio de primacía de la realidad (art. V.8) y la buena fe (art. V.5), presentes en la tutela el consumidor, no hacen sino desenmascarar la situación que el banco prefiere que quede oculta o que se siga en la ficción legal de que los contratos de adhesión se "negocian y se pactan". En efecto, no debe primar el ropaje legal del contrato, sino la operación económica[17], la realidad de la relación de consumo, las circunstancias del acto de consumo, los riesgos reales de la actividad y quién está en mejores condiciones de asumirlos.

17 Gabrielli señala que la *operación económica* es una categoría unitaria y compuesta que comprende no solo al reglamento (texto del contrato), sino a todos los comportamientos vinculados con él para la consecución de los resultados perseguidos, y también la situación objetiva en la cual las reglas y los otros comportamientos confluyen ("La operación económica en la teoría general del contrato", *Ius Et Veritas*, n.º 44, Lima: 2012, pp. 24-25).

Lo que prima es la efectiva tutela que la Constitución otorga al consumidor.

6. El *phishing* es uno de los riesgos operacionales típicos de la actividad bancaria

En otro trabajo[18] hemos tratado la incidencia de la gestión de los riesgos bancarios y en particular del riesgo operacional[19], en los múltiples daños que se generan en su actividad. Pues bien, consideramos, adelantando una conclusión, que el *phishing,* así como otros fraudes electrónicos, constituyen riesgos de la actividad bancaria del tipo operacional que se presentan en la plataforma de servicios por Internet, es decir, eventos de pérdidas bancarias originados en la tecnología de la información (fallos en la seguridad de sus sistemas) y eventos externos (fraudes de terceros).

Sostenemos que son las reglas expedidas por el Comité de Basilea en materia de riesgo operativo las que resultan aplicables en materia de responsabilidad del profesional bancario respecto del consumidor.

En cuanto a la peligrosidad de la actividad bancaria, es pertinente destacar que los múltiples daños que nos muestra la cada vez mayor casuística en torno a ella, revelan, en esta sociedad del riesgo, que en tanto como ninguna otra actividad el dinero es su elemento principal, queda ella expuesta a la delincuencia tradicional y no tradicional como la delincuencia cibernética. Los hurtos, los robos, las estafas son un constante riesgo de la actividad bancaria, riesgos típicos, como estamos viendo, que deben ser rigurosamente gestionados para evitar los daños al cliente bancario o consumidor. La banca, en su condición de experta, tiene que estar un paso más allá en la prevención de los daños, daños además que tiene la obligación de conocer, medir y gestionar.

En cuanto a la pericia exigible a los bancos, ya está dicho que ellos son agentes expertos que tienen el conocimiento técnico para desarrollar sus actividades, cumpliendo las reglas de su profesionalidad, de modo que le son reprobables las conductas que suponen una ausencia del empleo de esos cuidados mínimos para realizar su actividad.

Finalmente, en cuanto al costo de las medidas de precaución, es el banco el mejor ubicado para, primero, identificar el riesgo de daños, segundo, gestionarlos y tercero, trasladarlos a los precios de sus servicios. Su condición de experto lo

18 Campos Bermudez, *La responsabilidad civil de los bancos en compras financiadas en planos de inmuebles y en operaciones por Internet*, ob. cit.

19 La Resolución SBS N.° 2116-2009, del 2 de abril del 2009, aprobó el Reglamento para la Gestión del Riesgo Operacional, aplicable para todo el sistema financiero peruano, y cuyo art. 3 lo define como "la posibilidad de ocurrencia de pérdidas debido a procesos inadecuados, fallas del personal, de la tecnología de información, o eventos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y de reputación […]. Las empresas deben realizar una gestión adecuada del riesgo operacional que enfrentan, para lo cual observarán los criterios mínimos indicados en el presente Reglamento".

Número 52 • Octubre 2018 • pp. 277-302
ISSN 2313-4828 (impresa) • ISSN 2415-2277 (en línea)

lleva a asumir los costos de precaución e incorporarlos al mercado a través de sus precios, es decir llevar a cabo lo que Franzoni denomina proceso de socialización de los costos de los daños[20].

Es importante también, para afrontar este problema de investigación, darle relieve a lo que se ha denominado la ética de la gestión de riesgos, es decir el reconocimiento de que los diversos riesgos afectan no solo a la bancos, sino a todos los integrantes de la sociedad, por lo que su identificación y tratamiento debe pasar al ámbito de las empresas quienes serán las responsables de la gestión, con miras a evitarlos o reducirlos, trasladarlos, cubrirlos y mantener aquellos que forman parte de la actividad de la empresa o no pueden evitarse o trasladarse.

7. Posición de Indecopi frente a este riesgo típico de la actividad bancaria

Dos preguntas nos ayudarán a centrar el tema: ¿son los fraudes electrónicos hechos desconocidos para los bancos o más bien riesgos típicos o frecuentes de su actividad? y ¿quién los conoce más, el banco o el consumidor? Ya vimos en el acápite anterior que el *phishing* sí es un riesgo típico de la actividad bancaria, pero la pregunta es por qué el Indecopi no los considera como tal y resuelve los casos considerando este elemento objetivo al momento de juzgar la diligencia o idoneidad del banco. De hecho, sus resoluciones adolecen de un registro moderno de la realidad actual, de las circunstancias en que se desarrolla estas operaciones y los riesgos que conllevan, sobre los cuales existe desde hace varios años una reflexión que tiene que ser compartida por los operadores del derecho.

En las resoluciones que emite el Indecopi resolviendo los múltiples casos que se denuncian, no se considera que el *phishing* sea un riesgo de la actividad bancaria. Siendo así, la perspectiva de solución que tiene es errónea. En la mayoría de tales resoluciones ni siquiera se identifica que se está en presencia de este tipo de fraudes bancarios. Solo le ha interesado al Indecopi, en una demostración de chato positivismo, que, si se verifica que la operación se registró en el sistema bancario con el empleo de los números de cuenta, clave y contraseña, la operación se reputa efectuada y de este modo se cumple con los estándares de idoneidad exigidos.

No entiende el Indecopi que precisamente esos estándares de idoneidad que tiene establecido en sus resoluciones como precedentes[21] no son los correctos,

20 Franzoni, Massimo, "La evolución de la Responsabilidad a partir del análisis de sus funciones", en *Responsabilidad Civil Contemporánea*, Lima: Ara Editores, 2009, p. 38.

21 Resolución Final N.º 0604-2015/PS2 (Exp. N.° 0901-2012/PS2), del 23 de junio del 2015. En ella se resolvió: "declarar infundada la denuncia… por infracción de los artículos 1 literal c), 18 y 19 de la Ley N.° 29571, del Código de Protección y Defensa del Consumidor, en virtud a que ha quedado evidenciado que las transacciones efectuadas entre el 26 al 29 de julio de 2012, por las sumas de S/. 1379,78; S/. 2975, 37 *(3 operaciones por las sumas de*

S/. 991,79) y S/. 5,28 con cargo a la Tarjeta Multired de la señora Landa, se autorizaron válidamente [...]".

Resolución Final N.º **0227-2015/PS2 (Exp.** N.° 2370-2014/PS2), del 26 de febrero de 2015. En ella se destaca que "[…] el hecho que el interesado haya puesto en conocimiento del Banco que se le envió un correo electrónico con un supuesto *link* para realizar la actualización de sus datos personales, no quiere decir que la entidad financiera se encontrara obligada a tener en observación su(s) cuenta(s). La finalidad para la cual el denunciado le requirió que reenviara el correo electrónico señalado en el párrafo anterior fue poder verificar las direcciones electrónicas desde las cuales se solicitaba información que únicamente debía ingresar a través del portal web del Banco y tomar acciones internas respecto a éstas […]".

Resolución Final N.º **0711-2015/PS2 (Exp.** N.° 0573-2015/PS2), del 17 de julio de 2015. En ella se defiende la posición del banco de trasladar el riesgo de estos fraudes electrónicos al consumidor: "[…] en la medida que en el presente caso no se ha configurado un supuesto que ameritara el reporte ante el Banco de la pérdida, robo o extravío de la tarjeta de coordenadas, sobre la realización de alguna operación o situación ajena al consumidor respecto a su cuenta de ahorros, la entidad financiera no podía haber tomado medidas de prevención en caso se efectuaran transacciones que no fueran reconocidas por el consumidor […] De acuerdo a ello y, como el mismo consumidor ha señalado, cabría la posibilidad que las operaciones pudieran haber sido realizadas bajo un fraude informático, el cual se pudo llevar a cabo, por ejemplo, con un virus troyano en su computador, sin que ello pudiera ser de responsabilidad de la entidad financiera ya que, la misma se encarga que se cumpla con las medidas de seguridad requeridas para cada tipo de operación y no podía de prever que el consumidor tomara o no las medidas de precaución respecto de los aparatos tecnológicos (laptop, computadora, ipad, ipod) que utilizara para llevar a cabo operaciones como las que cuestiona […]".

Resolución Final N.º **0987-2015/PS2 (Exp.** N.° 0953-2015/PS2) del 23 de septiembre de 2015. En ella se insiste en la falta de diligencia del consumidor: "[…] si bien la entidad financiera debe contar con un mecanismo que garantice la seguridad de dichas transacciones, corresponde al consumidor adoptar una conducta diligente a fin de que el equipo informático utilizado para sus operaciones se mantenga dentro de los parámetros advertidos por las entidades financieras para mitigar los riesgos derivados de la utilización de Internet (no utilizando cabinas públicas ni redes inalámbricas, a través de utilización y actualización constante de antivirus, *antispyware*, *antirootkits* y *firewalls*, entre otros); pues de lo contrario, la falta de medidas de precaución neutralizaría todas las medidas de seguridad adicionales a ser adoptadas por el Banco […] De acuerdo a ello, y como el mismo consumidor ha señalado, en el supuesto de que las operaciones pudieran haber sido realizadas bajo un fraude informático, ello no constituye una factor que atribuya responsabilidad a la entidad financiera en la medida que si bien dicha entidad es la encargada de que se cumplan las medidas de seguridad requeridas para cada tipo de operación, no podía prever que el consumidor adoptara o no las medidas de precaución necesarias para llevar a cabo operaciones como las que cuestiona […]".

Resolución Final N.º **0624-2015/PS2 (Exp.** N.° 0439-2015/PS2), del 30 de junio del 2015. En ella se impone al consumidor la prueba de que el *link* al cual accedió el consumidor era del banco: "[…] la denunciante, con anterioridad a la realización de la operación cuestionada, ingresó a un link que habría sido proporcionado por el Banco para actualizar los datos de su cuenta, para lo cual ingresó su número de tarjeta, DNI y las claves de seguridad; siendo que inmediatamente después tomó conocimiento de la transferencia a favor de un tercero. Partiendo de este hecho, se aprecia que la denunciante proporcionó información de su cuenta y de sus claves […] Asimismo, no aportó medio probatorio que acredite que la dirección electrónica a la que fue derivada para la actualización de los datos de su cuenta, correspondieran a los servidores del Banco; por lo que ahora no puede pretender trasladar la

Número 52 • Octubre 2018 • pp. 277-302
ISSN 2313-4828 (impresa) • ISSN 2415-2277 (en línea)

dado que no se ajustan a la realidad de la operación y a las circunstancias de esta especial relación de consumo en la que el riesgo es un factor fundamental. Y es que, como hemos señalado líneas atrás, con el desarrollo de la tecnología y el uso del ciberespacio, se han incrementado los riesgos y estos están cada vez presentes entre nosotros, pero no ha habido un adecuado tratamiento jurídico que esté a la altura de su gestión.

El Indecopi no ha reflexionado sobre la explicación acerca de que cómo es posible que existan operaciones que son validadas por los bancos pero que el cliente asegura no haberlas realizado. No le ha interesado al Indecopi identificar que existe una brecha en el sistema que permite que se lleven a cabo las operaciones fraudulentas aun cuando los clientes afirmen no haberlas realizado.

La conclusión del Indecopi es que fue el cliente el que permitió la injerencia de un tercero, que, contrariamente a la moderna gestión de riesgos que se viene desarrollando en el derecho financiero, es el cliente el que no gestionó sus riesgos y que deben pesar sobre él, las medidas de prevención. Semejante posición, por supuesto, es anacrónica e injusta. Como lo desarrollamos líneas atrás, frente al riesgo de daños, en el proceso de socialización de las pérdidas es la empresa la que está en mejores condiciones de prevenirlos, asumirlos y trasladarlos en sus precios a todos los consumidores.

En el caso de los bancos, consideramos que el costo de las pérdidas por estos daños, están incorporados en el cobro de sus intereses, los cuales son bastante altos en comparación con otros países. Es decir, son los bancos y no el consumidor los que deben asumir esas pérdidas porque ya están incorporadas en los intereses que cobran.

IMPORTANTE

Para el Indecopi, el parámetro de idoneidad del banco en este tipo de operaciones vía Internet es la verificación de los mecanismos de seguridad implementados por los bancos, pero el problema es que, para tal verificación representativa de la "idoneidad" del banco, se identifica, erróneamente a nuestro juicio, la seguridad en la operación con la sola digitación de los datos y claves. De tal modo, verificados que estos fueron digitados, el Indecopi considera válida la operación.

8. La obligación legal bancaria de gestionar el riesgo de phishing

La gestión de riesgos en la actividad bancaria es una obligación legal que se incorpora al juicio de su diligencia profesional. No forma parte de una política de buenas prácticas de carácter voluntaria. Dicha obligación no debe ser ajena a los operadores del derecho, pues constituye una conducta típica exigida por la ley y exigible desde luego por los consumidores afectados.

responsabilidad del proceso de la operación hacia su proveedor […]".

La verificación de su incumplimiento o cumplimiento inadecuado tiene la aptitud para fundar un caso de responsabilidad civil, no como criterio de imputación objetivo, sino como parte del juicio de su diligencia profesional, un juicio ciertamente más empoderado, con más capacidad y fuerza de actuación para procurar la condena de responsabilidad al banco. En ese sentido, el juicio de responsabilidad civil de las entidades financieras debe tomar en cuenta su obligación de gestión de los riesgos de su actividad.

Nosotros sostenemos que, en nuestro país, los bancos no están cumpliendo sus obligaciones legales, y que si ellos han registrado un crecimiento en sus utilidades como se ha reconocido, esto se debe a que en parte no están asumiendo pérdidas que se están quedando hoy en la esfera de los consumidores y clientes bancarios.

Ahora bien, siguiendo la posición del profesor Fernández, que plantea que la diligencia llega hasta donde comienza la imposibilidad de modo que solo ella libra al deudor[22], tenemos que también en estos casos de fraude por Internet o *phishing* el banco solo podrá liberarse del cumplimiento de sus obligaciones, una de las cuales es la gestión de los riesgos de su actividad, si prueba el caso fortuito o la fuerza mayor, es decir, que acontecimientos extraordinarios, imprevisibles e irresistibles les impidieron cumplir sus obligaciones, derivadas de los contratos de cuenta de ahorros o de tarjeta de crédito.

Del primero deriva una obligación de custodia de los fondos dinerarios depositados en el banco, y del segundo una obligación de entrega de recursos dinerarios para atender las necesidades de compra del titular a su solicitud.

Pues bien, tales acontecimientos extraordinarios, imprevisibles e irresistibles que impidan al banco satisfacer su obligación de custodia y con él, el interés del acreedor, no son probados por los bancos en los casos que ha conocido el Indecopi. Le ha bastado hasta ahora, erróneamente, a sus tribunales administrativos que el banco pruebe con sus propios reportes de sus sistemas operativos que las transacciones bancarias se realizaron empleando las claves respectivas. Para el Indecopi en la probanza de ello consiste su diligencia, sin considerar que existe una obligación legal de gestionar los riesgos típicos de su actividad, uno de los cuales es precisamente el fraude electrónico de *phishing*.

Lo que estamos planteando aquí en respuesta a esa deficiente solución al problema por parte del Indecopi (que lejos de resolverlo lo agudiza, dado que el cliente se queda peor de lo que estaba porque tienen que asumir los pagos de la defensa que emplea en su reclamo), es que tan solo verificando que se omitió

22 Fernández Cruz, Gastón, "El deber accesorio de diligencia y la responsabilidad derivada del incumplimiento en las relaciones obligatorias", en *Negocio jurídico y responsabilidad civil. Estudios en Memoria del profesor Lizardo Taboada Córdova*, Lima: Grijley, 2004, p. 617.

Número 52 • Octubre 2018 • pp. 277-302
ISSN 2313-4828 (impresa) • ISSN 2415-2277 (en línea)

cumplir o se cumplió defectuosamente la obligación de gestionar el riesgo de *phishing*, riesgo típico de su actividad, como hemos sostenido, podremos encontrar el fundamento para establecer la responsabilidad de los bancos.

Y es que, dada su posición de preeminencia lograda por su experiencia y conocimientos en el campo de sus operaciones, los bancos, a diferencia de los consumidores profanos, gozan de la suficiente capacidad para administrar los riesgos inherentes a su actividad profesional y precaver los daños que la misma conlleva. Por eso, como estamos planteando, su culpa, como criterio de imputación, debe analizarse dentro de las posibilidades de actuación con que cuentan.

En este orden de ideas, el contenido del deber de diligencia que les es impuesto, está integrado, como hemos dicho antes, por los postulados de la llamada *lex artis*, de donde se desprende, entre otras cosas, la obligación de gestionar los riesgos operacionales como el *phishing*.

El tomar en cuenta estos conceptos de la gestión de riesgos para la determinación de la responsabilidad civil de las entidades financieras es un manifestación concreta de la visión estratégica del derecho, de esa estrategia de *repensamiento* del derecho civil que nos propone De Trazegnies[23], de esa estrategia eficiente del conocimiento del "conjunto de la realidad" a la que el derecho debe adaptarse.

La actividad bancaria, como hemos visto, acarrea riesgos y como estos tienen que ser asumidos o distribuidos, no son sino los bancos los llamados a incorporarlos en sus precios (los intereses) o asegurarlos, pues están en mejores condiciones que sus clientes consumidores. Son los bancos los que están en mejores condiciones de prevenir los daños, de trasladar los costos de éstos a los precios (los intereses y comisiones) y eventualmente de asegurarlos como lo plantea la doctrina civil moderna y la propia legislación financiera.

9. ¿Existe una obligación de custodia ex recepto del banco?

Son tradicionalmente hipótesis de responsabilidad *ex recepto* en la legislación italiana (de la que la nuestra es tributaria, como sabemos, en materia de contratos y responsabilidad civil), la responsabilidad del hospedante por la destrucción, deterioro o sustracción de las cosas llevadas por el cliente al albergue, la de los almacenes generales por la conservación de la mercaderías depositadas y la del banco, en relación con el servicio de cajas de seguridad, por la idoneidad y custodia de los locales y por la integridad de la caja.

Se sostiene, en la doctrina y legislación italiana[24], que de esta obligación

23 De Trazegnies, Fernando, "El Derecho Civil ante la post-modernidad", en *Derecho Pucp,* n.° 45, Lima: 1991, pp. 313, 329 y 332.

24 D'amico, Giovanni, *Contribución a la teoría de la responsabilidad contractual*, Lima: Legales Instituto, 2015, p. 11 y ss.

ex recepto deriva una forma particular de responsabilidad por incumplimiento que, según la opinión común, resultaría "agravada" respecto del esquema ordinario, porque supone una carga probatoria más severa al deudor, a quien se le exige no solo la prueba de la diligencia sino la prueba *positiva* del hecho que ha causado el incumplimiento.

Pues bien, *aggiornando* tal noción de obligación *ex recepto* y siguiendo la referida doctrina, consideramos que sí es posible sostener que existe una obligación de custodia *ex recepto* del banco sobre los fondos dinerarios de los clientes depositados en él, dado el progreso de los riesgos bancarios a los que hemos hecho referencia antes y su presencia en las nuevas formas de relación entre el banco y sus clientes, como la banca por Internet.

Esta agravación de responsabilidad consiste en la asignación al deudor del *riesgo de las causas* "*ignotas*", de las que él respondería incluso si probase haber sido diligente[25]. En tal supuesto, por ello, no bastaría la demostración genérica de haber adoptado la diligencia necesaria, sino que sería necesaria la identificación concreta del evento que ha tornado imposible la prestación. En el caso de *phishing* esto supone la certeza de que tal evento ha ocurrido y no que se "presuma" que la operación la efectuó el consumidor.

Este facilismo, que avala una mala lectura de la legislación nacional por el Indecopi, impide que se transparente la real dimensión del riesgo de la plataforma de la banca por Internet y que se planteen las soluciones adecuadas acorde con la obligación del banco de gestionar tales riesgos dada su condición de empresa experta y la concreta obligación de custodia que emana de los contratos de depósito.

IMPORTANTE

Cabe añadir que uno de los propósitos del Código de Consumo contemplado en su artículo II es la corrección de conductas y prácticas que afecten los legítimos intereses de los consumidores. Esta función correctora alude a un estado de anormalidad que puede presentarse en una relación de consumo por conductas (incumplimientos) o prácticas (contratos de adhesión, abuso de posición de dominio, exclusión de responsabilidad, indebido reparto de riesgos, etc.) que afectan los intereses legítimos de los consumidores.

De acuerdo con la doctrina italiana, cuando el artículo 1218 del *Códice* (entre nosotros, el art. 1317) alude a la locución *causa no imputable*, obliga al deudor a probar los dos elementos de que ésta se compone; esto es, primero probar la causa, el *phishing* en este caso, y luego probar la no imputabilidad, es decir, que la ocurrencia de tal evento no pudo ser evitado por el banco por ser

25 *Ibid*. pp. 39-40.

Número 52 • Octubre 2018 • pp. 277-302
ISSN 2313-4828 (impresa) • ISSN 2415-2277 (en línea)

extraordinario, imprevisible e irresistible. En esta posición, en buena cuenta, la prueba de la causa no imputable equivale a la prueba del caso fortuito yo la fuerza mayor, de forma tal que el deudor bancario, siempre deberá soportar la responsabilidad de las *causas ignotas*.

Así las cosas, el banco solo podrá liberarse con la específica prueba *positiva* de que el daño fue causado por un evento ciertamente *identificado* y del todo *extraño* a sí mismo. Esto supone la necesidad de que demuestre la específica *causa* (no imputable) que le ha impedido el cumplimiento, con la consecuente atribución del riesgo de la *causa ignota* a él. Esta doctrina enfatiza por eso que "será sólo luego de que el deudor haya probado la *causa* concreta del incumplimiento, que se podrá pasar a la evaluación de la diligencia por el prestada"; de este modo, "la determinación de la causa sirve sustancialmente para brindar el objeto del juicio de no imputabilidad, que en caso contrario quedaría suspendido en el vacío, carente de un plazo material de referencia"[26].

La referida doctrina, que entre nosotros ha sido asumida por el profesor Fernández, como ya anotamos, identifica la "objetividad" de la responsabilidad por inejecución de obligaciones con la noción de imposibilidad absoluta y objetiva de la prestación. Nos explicamos. Esta postura considera que el deudor debe responder por el incumplimiento a menos que la prestación sea absoluta y objetivamente imposible, independientemente de la diligencia del deudor, quien solo podrá liberarse de su responsabilidad probando la causa extraña, esto es, el caso fortuito o la fuerza mayor.

Ahora bien, si alineamos la obligación ampliada *ex recepto,* como la que recae en el banco, con la obligación de gestionar los riesgos inmanentes de su actividad empresarial, veremos que tal riesgo profesional, del que hablamos líneas arriba, justifica la presunción que los daños son causados por el banco. Esta idea va en la línea de la presunción de responsabilidad de la culpa leve en la responsabilidad contractual, una culpa no identificada con la diligencia como conducta de mero esfuerzo, sino a una diligencia que equivale a la satisfacción del interés del acreedor, diligencia cuyo límite, como ha quedado anotado antes, es la imposibilidad.

10. Idoneidad de los bancos frente al *phishing*

En este tipo de situaciones jurídicas nosotros consideramos que la idoneidad de los bancos debe apreciarse en dos momentos. Uno *ex ante*, sustentado en el derecho del consumidor a una información suficiente y adecuada por parte de su proveedor (art. V.3, art. 1, art. 2 del Código de Consumo y art. 1362 del Código Civil); y otro *ex* post, sustentado en el derecho del consumidor a la seguridad en las transacciones en la relación de consumo (art. 1.g, art. 19, art. 20, art. 25, art. 26, art. 29 del Código de

26 *Ibid.*, pp. 47-49.

Consumo y art. 1362 del Código Civil). El primero referido a la información especializada y suficiente que debe brindar el banco sobre los riesgos de usar su canal de atención de banca por Internet. Y el segundo referido a las medidas de seguridad que debió tomar para detectar las operaciones fraudulentas y evitar que estas culminen su fase criminal con su cobro a través de otras cuentas del mismo banco.

10.1 La obligación de informar adecuadamente

La gran cantidad de casos de *phishing* son demostrativos que los bancos no cumplen con informar suficientemente y de manera concreta a sus clientes respecto de los riesgos que implica hacer operaciones en la banca por Internet. Información que debe ser especial, de manera expresa y autónoma, tanto más si muchos clientes no están familiarizados con la tecnología y sus riesgos. Todo lo contrario, lo único que en general hace el banco es empujar a sus clientes a utilizar su plataforma de Internet, es decir, su producto banca por Internet, por sus "ventajas y maravillas", sin que exista información proporcional y suficiente acerca de los peligros de este canal de atención.

Si bien el Internet ha facilitado mucho la difusión de la información y el conocimiento, no cabe duda de que puede engendrar riesgos y peligros que provocan condiciones de incertidumbre, no solo en las personas, sino también en las empresas que se sirven de ella. Frente a estas condiciones, se considera que es bastante claro que quien posea mayor información estará en capacidad de predecir con mayor exactitud el riesgo involucrado en una transacción[27].

La información implica costos y ya hemos visto que los bancos buscan siempre evitarlos, por eso promueven su banca por Internet; pero dejan prácticamente solos a sus clientes, expuestos a los peligros de dicha plataforma de sus servicios. La inversión en publicidad que realizan los bancos sobre los peligros mencionados es sustancialmente menor a la que realizan para promover dicha plataforma. Nos preguntamos: ¿debe conocer el banco que estos fraudes existen?, ¿no es propio de su actividad reconocer que esto ocurre?, ¿no es necesario que el banco haga algo para que no ocurra?, ¿qué hace para evitarlo?

Algo que sin duda puede hacer es informar, pero informar lo suficiente, de manera proporcionada al interés e inversión con que publicita su canal de banca por Internet (TV, radio, etc.). ¿Lo hacen los bancos? No. ¿Remiten mensaje a sus clientes por correo electrónico advirtiéndoles de los peligros de la banca por Internet? Tampoco. Los bancos envían muchos mensajes invitando a la banca por Internet y muchos otros sobre sus múltiples productos y servicios, pero prácticamente ninguno sobre el peligro referido.

27 Haro Seijas, José Juan, "¿Periculum est dubitabilis? Algunas precisiones sobre el papel del riesgo en la contratación privada", *Themis,* n.º 49, Lima: PUCP, 2004, p. 191.

Número 52 • Octubre 2018 • pp. 277-302
ISSN 2313-4828 (impresa) • ISSN 2415-2277 (en línea)

Cabe recordar que el BCP reconoció que era bien caro atender en la ventanilla, por eso hicieron un esfuerzo para derivar sus clientes hacia canales alternativos como el Internet. Si, por ejemplo, revisamos la publicidad del BCP[28], observaremos que estos constantemente empujan a sus clientes a utilizar la plataforma de Internet para realizar operaciones bancarias. La razón de ello, como se dijo, y es legítima, es ahorrar costos, que la actividad bancaria sea más rentable. Empero, nos preguntamos: ¿qué hay del consumidor bancario?, ¿no estamos acaso expuestos los consumidores a una plataforma insegura sin que los bancos inviertan lo suficiente en información a sus clientes acerca de los peligros y las medidas de seguridad del empleo de esa plataforma a la que nos empujan?, ¿invierte lo suficiente los bancos en las medidas de seguridad de su sistema o canal de atención de banca por Internet?

9.2 La obligación de otorgar seguridad a sus transacciones

En relación con las medidas de seguridad, partamos por fijar la obligación del banco en esta materia. La Superintendencia de Banca y Seguros (SBS), mediante Resolución S. B. S. N.º 6523-2013, que aprobó el Reglamento de Tarjetas de Crédito y Débito (art. 18 inc. 6), dispone que los bancos deben: "Mantener sistemas informáticos y aplicaciones seguras; para el caso de software provisto por terceros, establecer procedimientos para identificar vulnerabilidades y aplicar actualizaciones; para el caso de desarrollos de sistemas propios, adoptar prácticas que permitan reducir las vulnerabilidades de seguridad de dichos sistemas".

Adicionalmente, el artículo 17, "Medidas de seguridad respecto al monitoreo y realización de las operaciones", establece:

> Las empresas deben adoptar como mínimo las siguientes medidas de seguridad con respecto a las operaciones con tarjetas que realizan los usuarios:
>
> 1. Contar con sistemas de monitoreo de operaciones, que tengan como objetivo detectar aquellas operaciones que no corresponden al comportamiento habitual de consumo del usuario.
> 2. Implementar procedimientos complementarios para gestionar las alertas generadas por el sistema de monitoreo de operaciones.
> 3. Identificar patrones de fraude, mediante el análisis sistemático de la información histórica de las operaciones, los que deberán incorporarse al sistema de monitoreo de operaciones.

Como vemos, la SBS exige a todas las empresas implementar controles específicos de seguridad, ya sea que se trae del uso de un software provisto por terceros o de desarrollo propio. Los bancos tienen así la obligación de implementar medidas para reducir las vulnerabilidades de seguridad en sus sistemas. Esta obligación debe ser concordada con la obligación de gestionar riesgos de su actividad y, en particular, los riesgos operacionales en sus modalidades de tecnología de la información

28 Revisar cita 9.

y fraudes externos, de los que hemos hablados líneas anteriores.

Ahora bien, si la modalidad del *phishing* es un patrón de fraude reiterativo, el banco tiene la obligación legal de realizar un análisis sistemático y tomar las medidas de seguridad pertinentes. Generalmente, estos tipos de fraudes son detectados por los bancos y por eso proceden a bloquear temporalmente las tarjetas. Las preguntas que surgen de ello son: ¿qué motivó esta decisión de los bancos de bloquear las tarjetas?, ¿qué mecanismos tienen para reconocer que esas transacciones eran sospechosas?, ¿si ya sabían que eran sospechosas por qué no bloquean el cobro a través de las otras cuentas del mismo banco?, ¿conoce el banco que la modalidad de fraude consiste precisamente en trasladar el dinero de una cuenta a otra? Por supuesto que lo sabe, pero su cómoda posición y la falta de reclamos (denuncias ante Indecopi o demandas ante el Poder Judicial) de los clientes, hace que no se sienta incentivado para tomar medidas que remedien o eviten estos fraudes.

Es incontrovertible que el banco tiene algún sistema que lo llevó a bloquear las tarjetas, pero otra relevante pregunta es: ¿por qué no lo hace antes que culminen las transacciones sospechosas? Esta falencia de detección oportuna del mecanismo de fraudes de los bancos demuestra que es deficiente, por lo que la pérdida o daño derivado de él constituye una indebida gestión de su riesgo operacional (riesgo de su actividad profesional), como lo hemos señalado líneas atrás.

Una gran corporación profesional como un banco no puede tener un sistema tan vulnerable o tan deficiente de no poder detectar en su oportunidad los fraudes y evitar que estos finalmente se lleguen a verificar en los hechos. Los bancos deben probar que sus sistemas de seguridad tienen costos prohibitivos que les impiden evitar que se generen estos tipos de fraudes, en los que se les instrumentaliza. Los bancos, por lo general con la venia de las autoridades en este sistema de "protección" al consumidor, no son requeridos a demostrar que la causa le sea extraordinaria, imprevisible e irresistible, como lo exigen los artículos 1315 y 1314 del Código Civil, sino simplemente se aplica las cláusulas de adhesión que perniciosamente trasladan el riesgo hacia los consumidores.

El servicio bancario, como decíamos, está sujeto a cláusulas generales de contratación, de manera que los adherentes consumidores no solo gozan del beneficio de interpretación favorable que contempla el artículo 1401 del Código Civil, y de la especial tutela de la legislación en materia de protección al consumidor, sino además de la protección constitucional que consagra su defensa (art. 65). No en vano en esta materia el Tribunal Constitucional ha reconocido los principios de deber especial de protección, principio de *pro* consumidor, principio de proscripción del abuso del derecho, principio de

Número 52 • Octubre 2018 • pp. 277-302
ISSN 2313-4828 (impresa) • ISSN 2415-2277 (en línea)

restitutio in integrum, principio *in dubio pro* consumidor.

IMPORTANTE

En cuanto a la peligrosidad de la actividad bancaria, es pertinente destacar que los múltiples daños que nos muestra la cada vez mayor casuística en torno a ella, revelan, en esta sociedad del riesgo, que en tanto como ninguna otra actividad el dinero es su elemento principal, queda ella expuesta a la delincuencia tradicional y no tradicional como la delincuencia cibernética. Los hurtos, los robos, las estafas son un constante riesgo de la actividad bancaria, riesgos típicos, como estamos viendo, que deben ser rigurosamente gestionados para evitar los daños al cliente bancario o consumidor. La banca, en su condición de experta, tiene que estar un paso más allá en la prevención de los daños, daños además que tiene la obligación de conocer, medir y gestionar.

Tanto el deber de prestación como el de seguridad conforman el deber de idoneidad (art. II y 18 del Código de Consumo). Sobre la idoneidad y las omisiones de las medidas de seguridad en operaciones bancarias, se viene pronunciando la doctrina:

> […] los servicios deben cumplir con su función para ser considerados adecuados, idóneos y de buena calidad. Ahora bien, ¿será que, si un tercero accede a los portales electrónicos y con ello causa un perjuicio al cliente, se está frente a un caso de falta de idoneidad? De acuerdo con lo expuesto, la respuesta es afirmativa, como quiera que corresponde al significado de lo que debe ser idóneo el estar ligada la adecuación del producto a la necesidad del cliente. Entonces, se concluye que el servicio no es adecuado, por lo tanto, no es idóneo ni apto29.

El banco es una entidad corporativa que conoce su negocio y sabe que no tener un sistema adecuado de detección de fraudes es un defecto de su procedimiento, una negligencia de la que se valen terceras personas para ejecutar sus fraudes.

11. Conclusiones

- El *phishing* es uno de los fraudes por Internet más complejos, masivos y peligrosos que se presentan en la industria bancaria, que consiste en la apropiación fraudulenta de la identidad digital de un cliente para realizar operaciones por Internet, transfiriendo los fondos de la cuenta de la víctima hacia las cuentas de otras personas denominadas muleros, que forman parte de la cadena delictiva, o para realizar compras o pagos por Internet con cargo a las tarjetas de débito o crédito de la víctima.
- Frente a las denuncias de los consumidores que alegan falta de medidas de seguridad de los bancos, estos señalan que aquellas consisten en el bloqueo preventivo de las tarjetas

29 Anaya Saade, Celina, "Riesgos en las transacciones electrónicas bancarias. Una carga que debe ser asumida por la banca", en *Revista Mercatoria,* vol. 11, n.° 1, Universidad Externado de Colombia: 2012, p. 299.

luego de efectuado el reporte de las operaciones no reconocidas y evitar así que ellas sigan utilizándose, y que las alertas o monitoreo de las operaciones se realizaban teniendo en cuenta la línea de crédito del cliente. Añaden, amparados en los contratos de adhesión, que es responsabilidad de los clientes la utilización de sus tarjetas, claves y contraseñas secretas, de modo que les es imputable cualquier operación que se realice con ellos en la medida que son sus únicos custodios, excluyéndose así la responsabilidad al banco. Para el Indecopi, el parámetro de idoneidad de las medidas de seguridad de los bancos lo constituye solo la acreditación por estos a través de sus reportes informáticos, de la digitación de los datos, claves y contraseñas.

- Cuando en su defensa los bancos invocan como conducta causante de los daños el que el cliente facilitara a los terceros sus claves secretas que debió mantener en custodia, expresa en realidad una falacia porque (i) en rigor no existe tal "entrega" si no solo la digitación de las claves en el contexto de una petición efectuada por quien se supone es el banco, el cual en tal circunstancia no califica como tercero; (ii) porque lo que debe primar en una relación de consumo es la tutela efectiva del consumidor, teniendo en cuenta realidad de la operación económica y no el ropaje legal del contrato de adhesión que solo representa una realidad recortada y una inadecuada repartición de los riesgos.
- El *phishing,* así como otros fraudes electrónicos, constituyen riesgos típicos operacionales de la actividad bancaria que se presentan en la plataforma de servicios por Internet, es decir, eventos de pérdidas bancarias originados en la tecnología de la información (fallos en la seguridad de sus sistemas) y eventos externos (fraudes de terceros), siendo así deben ser rigurosamente gestionados para evitar los daños al cliente bancario o consumidor.
- Si, como sostenemos, la diligencia llega hasta donde comienza la imposibilidad de cumplimiento y solo ella libra al deudor, en estos casos de fraude por Internet o *phishing*, el banco solo debería liberarse del cumplimiento de sus obligaciones, una de las cuales es precisamente la gestión de dicho riesgo, si prueba el caso fortuito o la fuerza mayor, es decir, que acontecimientos extraordinarios, imprevisibles e irresistibles les impidieron cumplir sus obligaciones de custodia de los fondos dinerarios depositados en el banco y de entrega de los recursos dinerarios para atender las necesidades de compra del titular.
- Indecopi no considera al *phishing* como un riesgo típico de la actividad bancaria. Sus resoluciones adolecen de un registro moderno de la realidad y circunstancias en que se desarrolla estas operaciones

Número 52 • Octubre 2018 • pp. 277-302
ISSN 2313-4828 (impresa) • ISSN 2415-2277 (en línea)

y los riesgos que conllevan, por eso la perspectiva de solución que tiene es errónea. Solo le ha interesado al Indecopi, en una demostración de chato positivismo, que, si se verifica que la operación se registró en el sistema bancario con el empleo de los números de cuenta, clave y contraseña, la operación se reputa efectuada, y de este modo se cumple con los estándares de idoneidad exigidos.

- Para el Indecopi, contrariamente a la moderna gestión de riesgos que se viene desarrollando en el derecho financiero, fue el cliente el negligente al permitir la injerencia de un "tercero", ubicando el riesgo de *phishing* y sus medidas de prevención en su esfera de control y no en la del banco. Esto significa que son los clientes bancarios los que están asumiendo el riesgo de las pérdidas por estos eventos.
- *Aggiornando* la noción de obligación *ex recepto,* y siguiendo la doctrina italiana, consideramos que es posible sostener que existe una obligación de custodia *ex recepto* del banco sobre los fondos dinerarios de los clientes depositados en él. En ese sentido, el banco deudor está obligado a probar la causa del *phishing* y la no imputabilidad de su ocurrencia, es decir, que no pudo evitarlo por ser extraordinario, imprevisible e irresistible. El banco solo podrá liberarse con la específica prueba *positiva* de que el daño fue causado por un evento de tales características.
- La idoneidad de los bancos debe apreciarse en dos momentos. Uno *ex ante*, sustentado en el derecho del consumidor a una información suficiente y adecuada por parte de su proveedor (art. V.3, art. 1, art. 2 del Código de Consumo y art. 1362 del Código Civil), sobre los riesgos de usar su canal de atención de banca por Internet, sobre todo si muchos clientes no están familiarizados con la tecnología y sus riesgos como sí lo están los bancos, en quienes el cliente confía dada su condición de experto. La inversión en publicidad que realizan los bancos sobre los peligros mencionados es sustancialmente menor a la que realizan para promover dicha plataforma.
- La idoneidad *ex post* consiste en las medidas de seguridad y controles específicos que a requerimiento inclusive de la SBS debe implementar. Los bancos tienen así la obligación de implementar medidas para reducir las vulnerabilidades de seguridad en sus sistemas. Si la modalidad del *phishing* es un patrón de fraude reiterativo, el banco tiene la obligación legal de realizar un análisis sistemático y tomar las medidas de seguridad pertinentes. Generalmente, estos tipos de fraudes son detectados por los bancos y por eso proceden a bloquear temporalmente las tarjetas, pero no evitan que se verifique el fraude con el cobro por terceros.

- Esta falencia de detección oportuna y evitación de su verificación con los retiros demuestra que el servicio del banco es deficiente. Los bancos deben probar que sus sistemas de seguridad tienen costos prohibitivos que les impiden evitar que se generen estos tipos de fraudes, en los que se les instrumentaliza. Los bancos, por lo general con la venia de las autoridades en este sistema de "protección" al consumidor, no es requerido a demostrar que la causa le sea extraordinaria, imprevisible e irresistible, como lo exigen los artículos 1315 y 1314 del Código Civil, sino simplemente se aplica las cláusulas de adhesión que perniciosamente trasladan el riesgo hacia los consumidores. 

12. Referencias bibliográficas

Agencia Efe, "El 98,5 de los riesgos bancarios en América Latina son informáticos". Recuperado de <https://bit.ly/2OwAfZE>.

Anaya Saade, Celina, "Riesgos en las transacciones electrónicas bancarias. Una carga que debe ser asumida por la banca", en *Revista Mercatoria,* vol. 11, n.° **1, U**niversidad Externado de Colombia: 2012.

Campos Bermúdez, José A., *La responsabilidad civil de los bancos en compras financiadas en planos de inmuebles y en operaciones por Internet*, Lima: Instituto Pacífico, 2018.

D'amico, Giovanni, *Contribución a la teoría de la responsabilidad contractual*, Lima: Legales Instituto, 2015.

De Trazegnies, Fernando, "El Derecho Civil ante la post-modernidad", en *Derecho Pucp,* n° 45, Lima: 1991.

El Comercio, "'Phishing' y 'bots': las amenazas al comercio en Latinoamérica". Recuperado de <https://bit.ly/2O1r1ow>.

El Comercio, "Las utilidades de los bancos crecieron 35% hasta setiembre". Recuperado de <https://bit.ly/2RjxadM>.

Espinoza Espinoza, Juan, *Acto Jurídico Negocial. Análisis doctrinario, legislativo y jurisprudencial*, Lima: Gaceta Jurídica, 2008.

Fernández Cruz, Gastón, "El deber accesorio de diligencia y la responsabilidad derivada del incumplimiento en las relaciones obligatorias", en *Negocio jurídico y responsabilidad civil. Estudios en Memoria del profesor Lizardo Taboada Córdova*, Lima: Grijley, 2004.

Franzoni, Massimo, "La evolución de la Responsabilidad a partir del análisis de sus funciones", en *Responsabilidad Civil Contemporánea*, Lima: Ara Editores, 2009.

Gabrielli, Enrico, "La operación económica en la teoría general del contrato", *Ius Et Veritas*, n.º 44, Lima: 2012.

Gestión, "Indecopi: 45 de cada 100 reclamos son contra entidades financieras", Recuperado de <https://bit.ly/2spFoWQ>.

Gestión, BCP, "Nuestra principal competencia no es otro banco, sino el dinero en efectivo". Recuperado de <https://bit.ly/2NloksF>.

Haro Seijas, José Juan, "¿Periculum est dubitabilis? Algunas precisiones sobre el papel del riesgo en la contratación privada", *Themis,* n.º 49, Lima: PUCP, 2004.

La República, "Vacían cuenta de ahorros clonando página web de entidad bancaria". Recuperado de <https://bit.ly/2QrMQua>.

Lampadia, "Fortaleciendo las capacidades de seguridad cibernética". Recuperado de <https://bit.ly/2H8WBZm>.

Perú 21, "Aumentan ciberataques en el Perú: ¿Por qué pensamos que nunca nos pasará a nosotros?". Recuperado de <https://bit.ly/2P3Yonc>.

RPP, "Cerca de 700 personas al mes son víctimas de fraude bancario". Recuperado de <https://bit.ly/2LN0KWe>.

Schiesaro, Diego Angelo, "El contrato asimétrico", *Actualidad Civil*, n.° 22, Lima: 2016.

Número 52 • Octubre 2018 • pp. 277-302
ISSN 2313-4828 (impresa) • ISSN 2415-2277 (en línea)