Título: La obligación de seguridad en las operaciones financieras con consumidores en la era digital. Con especial referencia a la problemática del phishing y del vishing
Autores: Arias, María Paula - Müler, Germán E.
Publicado en: SJA 14/07/2021, 14/07/2021, 43 -
Cita: TR LALEY AR/DOC/1657/2021

Sumario: I. Una aproximación inicial al problema.— II. Fenómeno sociológico de la vulneración de los sistemas bancarios.— III. La obligación de seguridad en las operaciones financieras.— IV. Herramientas procesales y de fondo que nos proporciona el ordenamiento jurídico argentino para hacer frente a la problemática del phishing o vishing.— V. Conclusión.

(*)

(**)

I. Una aproximación inicial al problema

Estamos atravesando la revolución digital. El uso masivo de Internet ha provocado una transformación que va más allá de lo tecnológico, hasta el punto de que el mundo actual muy poco tiene que ver con el que existía a principios de los noventa. Los hábitos de consumo se modifican fuertemente, desde los consumidores que aumentaron sus operaciones y trasladaron su vida completamente al entorno digital, hasta los que se vieron obligados a incursionar en él por primera vez (1). Para todos, el fenómeno se presenta muchas veces como insondable.

Internet es vivido y presentado por muchos como la "panacea", pues aumenta las posibilidades de interactuar con otros sujetos, de elegir productos y servicios en un rango cada vez más amplio y de disminuir el tiempo de elección, todo lo cual reduce drásticamente los costos de transacción en beneficio del consumidor (2).

La contracara de las nuevas tecnologías nos enfrenta a desafíos inéditos, que generan incluso un nuevo tipo de analfabetismo: el digital. Ya no se trata de no saber leer ni escribir, sino de carecer de las herramientas tecnológicas para poder realizar las tareas cotidianas. Si tradicionalmente se vinculaba al analfabetismo con el nivel socioeconómico o con la edad, lo novedoso del fenómeno digital es que puede afectar a todos, incluyendo a los propios nativos digitales. Ser analfabeto digital es grave: puede ser una limitante a la hora de obtener trabajo o una promoción, incluso ser parte de un grupo social (3).

Por ello, el principio protectorio debe manifestarse con toda su potencia (4). A las asimetrías tradicionales en la relación de consumo se suma una muy acrecentada desigualdad tecnológica, ya que en el medio virtual la diferencia cognoscitiva respecto del medio empleado es absoluta. La tecnología es cada vez más compleja, aunque se presente de modo simplificado frente al usuario, ocultando una gran cantidad de aspectos que permanecen en la esfera de control del proveedor. En consecuencia, puede afirmarse que la tecnología incrementa la vulnerabilidad de los consumidores, instaurando un trato no familiar (5).

Incluso podría plantearse como un tipo de hipervulnerabilidad, pues aún los más habituados y diestros usuarios de las nuevas tecnologías encuentran serias dificultades para comprender cómo funciona realmente el mundo virtual que utilizamos cotidianamente, hacer un uso racional y productivo de la red, distinguir lo verdadero de lo falso, proteger la información sensible.

De lo que no parece haber discusión es que todos los consumidores requieren en el entorno digital de una protección mayor a la que reciben en el mundo físico. Así, Tambussi destaca que "el sistema de comercio por medios electrónicos, lejos de atenuar la responsabilidad de los proveedores que lo utilizan, agrava sus obligaciones porque presupone el uso de una tecnología que exige un mayor conocimiento de su parte. En estos casos hay empresas que actúan profesionalmente y consumidores que no son expertos, en los que la distancia económica y cognoscitiva que existe en el mundo real se mantiene en el mundo virtual. Podríamos afirmar que no solo se mantiene, sino que se profundiza. Debe tenerse en cuenta también que la tecnología es cada vez más compleja en su diseño, pero se presenta de modo simplificado frente al usuario, ocultando de este modo una gran cantidad de aspectos que permanecen en la esfera de control del proveedor" (6). Wajntraub (7), citando a Sahián (8), así como a Chamatrópulos (9), también afirman que los consumidores electrónicos requieren de una tutela que se torna absolutamente necesaria (10).

La situación descripta generó, como no podía ser de otro modo, la aparición de nuevos modos de fraude. En este trabajo nos centraremos en dos de ellos, basados en ingeniería social, conocidos como phishing y vishing. Para caracterizarlos la jurisprudencia ha sostenido que el phishing consiste en un término informático que denomina a un conjunto de técnicas que persiguen el engaño de la víctima, ganándose su confianza, haciéndose pasar por una persona, empresa o servicio confiable (suplantación de identidad de tercero de confianza) para manipularla y hacer que realice acciones que no debería realizar (por ej. revelar información confidencial). Por

su parte, el vishing consiste en una de las innumerables formas de comisión del anterior, produciéndose el engaño a través de una llamada telefónica (11).

II. Fenómeno sociológico de la vulneración de los sistemas bancarios

Una nota del mes de febrero de 2021 (12) informa que en el lapso de solo seis meses tuvieron lugar un total de 270 millones de intentos de ciberataques en la Argentina. Uno de los sectores más damnificados del país fue el sector financiero, con 4 millones de ataques al día, de acuerdo con el Fortinet Threat Intelligence LATAM. Se informa que la oficina de Prevención de Fraude del Banco Santander ya destacaba que los dos principales ataques con los que lidiaron son las estafas telefónicas y las cuentas falsas en redes sociales. Evidentemente, es un problema muy conocido por las entidades bancarias (13).

Más allá de las diferencias en los métodos utilizados por los estafadores, lo que termina ocurriendo es que el consumidor desprevenido, confiando en la apariencia generada, entrega información de acceso a sus cuentas. Así, los engañadores obtienen no solo todo el dinero que hay en las cuentas, sino también los montos en concepto de préstamos que las entidades tienen preaprobados para sus clientes.

En el documento "Financial Consumer Protection Policy Approaches in the Digital Age" (14), producido por la fuerza de trabajo de protección al consumidor del G20/OECD, pueden encontrarse valiosas referencias sobre la enorme cantidad de consumidores que debieron volcarse a la contratación financiera online y a los múltiples riesgos que ello implica, no solo para los usuarios sino también para las instituciones.

Con relación a los fraudes sufridos por consumidores, aunque aclara que es imposible conocer todos los casos debido a la falta de denuncias, un informe de una dependencia de la Comisión Federal de Comercio de Estados Unidos de 2019 incluye 3.200.000 de reportes de fraudes y robo de identidad. Se advierte fácilmente que se trata de un flagelo mundial, que afecta incluso a los consumidores de los países más desarrollados, y por lo tanto más habituados y mejor preparados para enfrentarlo.

Esta realidad es la que llevó a la OCDE a redactar la Recomendación para la Protección de los Consumidores de Comercio Electrónico, requiriendo a los comercios que implementen sistemas de seguridad acordes con los riesgos generados, incluyendo aquellos relacionados con el acceso no autorizado o el uso de información personal, fraude y robo de identidad. De ese modo, se pone en cabeza del generador del riesgo la obligación de introducir métodos de seguridad más eficientes, sobre todo teniendo en que cuenta que, como destacó el Panel de Consumidores Financieros del Reino Unido, generalmente los consumidores no prestan un consentimiento informado, o cuando lo hacen, la mayoría no leen o no entienden las condiciones.

En Argentina las denuncias por estafas bancarias aumentaron un 3000% en la pandemia (15) y se cuentan por centenas, aunque también es un hecho que los números resultan inferiores a los reales ya que muchos optan por no denunciar o no saben cómo hacerlo.

El contexto de utilización de los servicios bancarios en general es fundamental para explicar el fenómeno. Los bancos cada vez tienen menos sucursales (16) y alientan u obligan a los clientes a operar a distancia: por teléfono, mail, redes sociales, etc. De ese modo, la utilización se hace cada vez más compleja, pues además de comprender el funcionamiento predispuesto del sistema del banco en cuestión, el usuario tendrá que poder distinguir en cada momento si está hablando con un representante del banco o con un impostor, lo que resulta imposible la mayoría de las veces (17). Esta situación es harto conocida por los bancos, que han verificado que las redes sociales permiten la realización de fraudes.

Nos proponemos, entonces, indagar el fenómeno —que se agravó con la pandemia— de las múltiples estafas que sufren los consumidores bancarios al ser contactados por estafadores que logran obtener datos del usuario (contraseña, token, etc.), acceder a las cuentas por medio del homebanking y operar haciéndose pasar por los clientes de los bancos (18).

III. La obligación de seguridad en las operaciones financieras

La primera regla que sienta el art. 42 de la Constitución tiende a la protección de su salud, seguridad e intereses económicos de los consumidores. Correlativamente, el art. 5º de la Ley de Defensa del Consumidor establece que "...las cosas y servicios deben ser suministrados o prestados en forma tal que, utilizados en condiciones previsibles o normales de uso, no presenten peligro alguno para la salud o integridad física de los consumidores o usuarios". A su turno, el art. 6º del mismo cuerpo legal dispone que "...las cosas y servicios,... cuya utilización pueda suponer un riesgo para la salud o la integridad física de los consumidores o usuarios, deben comercializarse observando los mecanismos, instrucciones y normas establecidas o razonables para garantizar la seguridad de los mismos".

Tal como puntualiza el voto del doctor Lorenzetti en un precedente de nuestro Máximo Tribunal (19) "...una vez calificada la existencia de una relación de consumo, surge un deber de seguridad de fuente constitucional

(art. 42, de la CN) y legal (arts. 5º y 6º, ley 24.240)". se desprenden con claridad dos grupos de deberes perfectamente diferenciados. El primero de ellos constituye un catálogo de medidas mínimas que obligatoriamente deben adoptar las entidades regidas por la norma, mientras que, lejos de agotarse allí el plexo de compromisos asumidos por estas instituciones, el restante grupo establece un deber de conducta indeterminado, sujeto a la específica ponderación de los riesgos previsibles, con base en los Estudios de Seguridad que habrán de efectuar estas instituciones, entre otras finalidades, "con el objeto de proteger a las personas", y cuya adopción queda "a exclusivo criterio y responsabilidad de las mismas".

De este modo, la obligación de seguridad en las relaciones de consumo está presente en toda la contratación bancaria con consumidores (20). Su incumplimiento supone la responsabilidad del banquero, salvo los supuestos de caso fortuito, fuerza mayor o culpa de un tercero por quien no debe responder. Para una valoración adecuada de estas eximentes es preciso considerar que la cuestión no es ajena al prestador del servicio, quien debe procurar por sí o por un tercero condiciones óptimas en materia de oportunidad, seguridad y confidencialidad (21).

Demetrio Alejandro Chamatrópulos (22) explica cómo ese deber de seguridad del banco para con su cliente se manifiesta al haberse sustituido el sistema de atención "humana" por el "automático": la entidad debe otorgar al cliente la misma seguridad que existe si la operación se hubiera hecho a través del primero. Explica el reconocido autor tucumano —en un comentario a fallo (23)— que el argumento se centra en el hecho que los actores hayan sido inducidos a error a través de un ardid, no significaba que estos debían hacerse cargo de las consecuencias dañosas, sino que ello debía ser soportado por el banco, con base en que las medidas de seguridad tomadas por este último fueron insuficientes para prevenir conductas engañosas como las que sufrieron los demandantes. No resulta en vano recordar que quienes han decidido la introducción de estas "máquinas" en el sistema bancario y, es más, quienes han promocionado intensamente su uso, son los mismos bancos. El hecho de que existan beneficios para ambas partes no nos debe hacer olvidar que el que decidió incorporar esta nueva tecnología fue el proveedor. Y se trata de una cosa claramente riesgosa y que en no pocas oportunidades experimentan fallas de diversa índole. El usuario simplemente tuvo que "acatar" el cambio en la manera de operar sin quedarle otra alternativa que aceptarla. Con base en ello, resulta indiscutible concluir que la entidad debe hacerse cargo de todos los riesgos que se derivan de la decisión tomada.

A los fines de evidenciar la contundencia con la cual se está evaluando esta obligación de seguridad, resulta ilustrativo traer a colación lo resuelto en el caso "Zappettini" (24) en donde se dijo que "la responsabilidad del banco es, desde el punto de vista del cliente, la que deriva de la existencia de una obligación de resultado en cuanto al correcto funcionamiento del sistema de cajero automático, evitando operaciones fallidas y permitiendo la permanente extracción de fondos o depósitos, la acreditación de pagos y transferencias sin error, la correcta consulta de saldos, etc. y, a la vez, de seguridad en cuanto debe brindarse al cliente una prestación funcional preparada para brindar el servicio de cajeros de la manera más confiable posible frente a maniobras fraudulentas de terceros".

En ese sentido, se ha sostenido en un comentario a fallo que se debe responsabilizar al banco por los daños y perjuicios provocados al titular de una tarjeta de crédito por la extracción de fondos por parte de un tercero, dado que, aunque el actor reveló a través de un familiar a una tercera persona su clave, ello no interrumpe el nexo causal como consecuencia del obrar negligente de la entidad financiera que no adoptó las medidas de seguridad adecuadas. En el caso comentado, el tribunal fundamentó su postura en la responsabilidad contractual que rige en el caso basándose en la obligación de seguridad de resultado (25).

En esta línea, es importante recordar que, en las Sextas Jornadas Bonaerenses de Derecho Civil, la Comisión N.º 2 presidida por el doctor Alberto Bueres concluyó que la obligación de seguridad es tributaria del principio de buena fe, es funcionalmente autónoma de la obligación principal e implica normalmente una obligación de resultado. Y dicha obligación de seguridad ha adquirido jerarquía constitucional en las relaciones de consumo a través del art. 42 de nuestra Carta Magna.

El BCRA ha reconocido los riesgos que implica la posibilidad de concretar contrataciones bancarias por medios electrónicos, dictando una serie de comunicaciones tendientes a proteger a los usuarios. La Comunicación "A" 6878 en el art. 3.8.5, dispone: "(...) Las entidades deberán prestar atención al funcionamiento de las cuentas con el propósito de evitar que puedan ser utilizadas en relación con el desarrollo de actividades ilícitas...". Asimismo, impone —en reiteradas oportunidades— la "implementación de mecanismos de seguridad informática que garanticen la genuinidad de las operaciones" (26).

Luego, mediante la Comunicación "A" 6017, concerniente a los "Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras", se destaca en el art. 6.3.2.1, que "[l]as entidades deben desarrollar, planificar y ejecutar un plan de protección de sus activos, procesos, recursos técnicos y humanos

relacionados con los Canales Electrónicos bajo su responsabilidad...", enumerando seguidamente, una serie de funciones y tareas relacionadas con los procesos estratégicos de seguridad para sus Canales Electrónicos, de conformidad con lo que surge del art. 6.3.2.2. Entre ellas, se ordena a las entidades adecuar los mecanismos implementados para la verificación de la identidad y privilegios de los usuarios, reducir la complejidad de uso y la maximización de la protección del usuario de servicios financieros, garantizar la trazabilidad completa de las actividades en un entorno seguro.

En su art. 6.7.4. resalta que "las entidades deben disponer de mecanismos de monitoreo transaccional en sus [canales electrónicos], que operen basados en características del perfil y patrón transaccional del cliente bancario, de forma que advierta y actúe oportunamente ante situaciones sospechosas en al menos uno de los siguientes modelos de acción: a. Preventivo. Detectando y disparando acciones de comunicación con el cliente por otras vías antes de confirmar operaciones. b. Reactivo. Detectando y disparando acciones de comunicación con el cliente en forma posterior a la confirmación de operaciones sospechosas. c. Asumido. Detectando y asumiendo la devolución de las sumas involucradas ante los reclamos del cliente por desconocimiento de transacciones efectuadas".

La normativa dictada por el BCRA ha sido ponderada por la jurisprudencia al valorar la obligación de seguridad que pesa sobre las entidades bancarias. Así, se sostuvo que "una de las obligaciones primordiales de los Bancos, que constituye el presupuesto de los servicios que ofrecen, es que estos sean brindados, tanto cuando se lo haga en forma personal como cuando lo sea por medio de elementos mecánicos o electrónicos, con total seguridad para el cliente. No está de más recordar que los servicios ofrecidos por cualquier Banco inciden directamente sobre el patrimonio del usuario, tanto en sus operaciones pasivas como en las activas..." (27).

Todo lo dicho resulta aplicable a las operaciones que comentamos. El sistema es diseñado e impuesto por las entidades financieras, sin que el cliente pueda más que confiar en que el banco tomará los recaudos para evitar estafas. Es el proveedor el que tiene el deber de tomar medidas adecuadas de seguridad, para prevenir y evitar el hecho delictivo.

La obligación de seguridad impone a la entidad arbitrar todos los medios para evitar que el riesgo inherente al sistema se concrete en un daño para sus clientes. Ante la ocurrencia de este, el banco solo podrá eximirse de responsabilidad probando la presencia de una eximente que tendrá que cumplir necesariamente con los requisitos de imprevisibilidad, inevitabilidad, ajenidad, etc. (28). La culpa o hecho de la víctima por lo general —y más allá de que la cuestión es casuística— no cumplirá con esos requisitos. Ya hemos destacado que para los bancos no se trata de hechos imprevisibles, sino por el contrario, muy conocidos. También se fue delineando la idea de que no son ajenos a su esfera de actuación ni resultan inevitables.

Existen tres grandes grupos de sistemas de validación de identidad: basados en lo que sé (por ejemplo, claves), en lo que tengo (por ejemplo, una tarjeta de coordenadas) o en lo que soy (por ejemplo, datos biométricos). Las entidades bancarias suelen utilizar el primero, que es el más inseguro. A veces recurren al segundo. Pero existen muchos otros, que exigen más pasos de verificación y son más eficaces. Pensemos en la firma digital: claramente no es suficiente con una simple clave. Si alguien inicia sesión en una de nuestras redes sociales en una computadora no habitual, el sistema nos alertará inmediatamente y si no fuimos nosotros, tendremos una vía expedita para evitar esa intromisión y el sistema impedirá el ingreso. Algunas plataformas utilizan una selfie o un video para la utilización de datos biométricos, etc. Los métodos que confían solo en el suministro de información (tarjeta de coordenadas, token, etc.) son ineficientes, pues si partimos de la hipótesis de que el usuario fue engañado y cree estar comunicado con la entidad, la mera advertencia de que no suministre datos carece de sentido (pues, insistimos, se tiene la convicción de estar en un ambiente seguro): sería necesario que el mensaje alerte, al menos, sobre el trámite que se estaría autorizando con ese código. Por ejemplo, si se informara que ese código se utilizará para autorizar un préstamo o una transferencia, el usuario podría notar el engaño. Si se tomaran medidas adecuadas el hecho dañoso sería evitable. Por ello se admite que el uso de la biometría como método de validación estará ampliamente estandarizado en un futuro (29).

En pocas palabras, es cuanto menos muy inseguro un sistema al que se accede con datos que el consumidor conoce. La peligrosidad del sistema es demasiado evidente y desde el punto de vista causal es determinante. El manejo irrestricto de la cuenta por el estafador no se produce porque el consumidor haya brindado los datos, sino porque el banco no toma más precauciones para asegurarse de la identidad del usuario.

Así pues, al realizar el análisis ex post facto para determinar la incidencia causal de las conductas del banco y de la víctima en la producción del daño (30), se puede concluir que, si el proveedor hubiera optado por un sistema más seguro, el daño no hubiera ocurrido, a pesar del hecho de la víctima. Este último sería inocuo, no pasaría de ser una condición o circunstancia incapaz de provocar el daño, pues los sistemas de seguridad lo hubieran evitado.

El sistema no es ajeno al banco, sino que es impuesto y diseñado por la entidad, forma parte de su esfera de acción (31). Entonces, el hecho de la víctima no reunirá los requisitos para eximir de responsabilidad en cuanto no se trata de un hecho exterior ajeno a la explotación, a las actividades, a las cosas de propiedad del deudor, a la obligación de seguridad (32).

El otro aspecto en el que la entidad debería tomar más precauciones tiene que ver con una segunda instancia de la estafa, en la que el impostor realiza actos a nombre del usuario. Resulta fácil para la entidad bancaria detectar e impedir actos irregulares.

Por lo general se producen varios sucesos sospechosos en pocos minutos. Se cambian todos los datos de seguridad de la cuenta, como la dirección de correo electrónico y el número de teléfono a los que se enviarán mensajes de alerta. Entonces, estos ya no serán recibidos por el usuario sino por el impostor. Y como ello se puede hacer con los mismos datos que el estafador ya obtuvo del consumidor, el que debería ser el segundo nivel de verificación (el mensaje de alerta) queda desmantelado al superar el primer nivel.

Asimismo, el hecho que el ingreso se produzca desde un equipo y una ubicación que no es la habitual puede ser detectado fácilmente por los sistemas, igual que la registración de operaciones poco habituales en escaso tiempo —por ejemplo, la solicitud de un préstamo y las transferencias de grandes sumas de dinero— deberían generar alertas para el banco, que por lo tanto debería verificar si realmente emanan del cliente y bloquearlas cuando no sea así. Entonces, nuevamente, el hecho de que el cliente haya brindado un par de datos no es causa suficiente y eficiente para la producción de la estafa, que no se podría concretar si la entidad bancaria cumpliera adecuadamente su obligación de seguridad y de prevenir los riesgos intrínsecos del sistema.

De este modo, se admitió la demanda contra el banco por considerar que no logró demostrar haber cumplido frente al cliente usuario del servicio de interbanking su deber de seguridad, así como tampoco con su obligación de suministrar toda la información, chequeos, verificaciones o cualquier otro elemento que razonable y suficientemente respaldara la operatoria de este medio telemático para comprobar y solucionar a la mayor brevedad la apuntada irregularidad. Incluso, la entidad bancaria había advertido —al ponerse en contacto con la actora— que algo no era habitual y, más aún, procuró el inmediato recupero de los fondos sin éxito, para luego en el proceso no efectuar actividad probatoria alguna tendiente a demostrar cuales fueron las causas que la llevaron a efectuar dichas advertencias (33).

IV. Herramientas procesales y de fondo que nos proporciona el ordenamiento jurídico argentino para hacer frente a la problemática del phishing o vishing

Frente al fenómeno del phishing o vishing en el marco de las operaciones financieras en el entorno digital, es necesario indagar respecto las herramientas procesales y de fondo que nos proporciona nuestro ordenamiento jurídico para dar respuesta satisfactoria a esta problemática.

En este sentido, frente a la gran cantidad de conflictos suscitados se han planteado acciones judiciales con finalidades diversas. Algunas de ellas tienden a declarar la nulidad de los créditos otorgados fraudulentamente; otras tienen por finalidad prevenir o evitar el agravamiento de los daños ya irrogados; en otros supuestos tienen por objeto la reparación de los daños y perjuicios ocasionados e incluso, algunas pretensiones tienden a sancionar conductas de la entidad bancaria que denotan un grave menosprecio a los derechos del consumidor o usuario de servicios financieros.

IV.1. Tutela inhibitoria o preventiva

En el derecho civil surge la tutela inhibitoria con una serie de instrumentos que permiten prevenir el daño antes de que se produzca, incursionando en el orden social al señalar conductas obligatorias. La tutela inhibitoria —que siempre tiene una finalidad preventiva— admite, como género, dos especies: una acción cautelar que es provisoria y otra definitiva, las que se diferencian en su instrumentación procesal, unidas ambas en su finalidad preventiva de impedir la concreción de la amenaza del daño, frente al interés —legítimo o simple— del titular requirente (34). Es decir, lo que diferencia los supuestos es el tiempo: en la vía cautelar se debe probar el peligro en la demora, en la tutela definitiva la amenaza de daño; lo cautelar recae sobre el bien a asegurar y la tutela preventiva y las medidas autosatisfactivas sobre la prestación; pero todas tienen en común la prevención del daño (35).

En el marco de la problemática del phishing o vishing existe la posibilidad de encausar la tutela preventiva a través de acciones individuales o incluso mediante una acción colectiva preventiva autónoma consagrada en los arts. 1711 y ss. del Cód. Civ. y Com. y que tenga por objeto que se cumplimente adecuadamente la obligación de seguridad que pesa sobre las entidades bancarias para evitar que se produzcan nuevos daños o impedir su continuación por estafas como las relatadas precedentemente. Así, la pretensión preventiva (arts. 1710 a 1713, 1032 y cc. del Cód. Civ. y Com.) constituye: una pretensión típica y autónoma; de derecho sustancial; definitiva

o provisoria; principal o accesoria; despachada de oficio o a pedido de parte; mediante la cual se regula el deber legal de impedir la producción del daño y el de evitar o disminuir su continuación o agravamiento (36).

Al respecto cabe tener presente que la invocación y prueba de la existencia de la obligación de seguridad en este ámbito puede constituir un elemento dirimente para el despacho de medidas inhibitorias, particularmente, de carácter cautelar o autosatisfactivo. El interés en la prevención del daño que condiciona la legitimación activa del acreedor (art. 1712, Cód. Civ. y Com.) y la razonabilidad de las medidas que se adopten, en función de las circunstancias del caso y de la propia economía del contrato, tornan insoslayable la previa ponderación de estos aspectos (37).

Por otro lado, como una manifestación de la tutela inhibitoria se encuentra el otorgamiento de medidas cautelares tendientes a evitar el agravamiento de los daños ocasionados respecto de aquellos usuarios que se han visto afectados por estas estafas. De este modo, la mayoría de las medidas cautelares que se han otorgado son medidas de no innovar o innovativas (38) —según el caso—, tendientes a que la entidad bancaria se abstenga de cobrar los préstamos que se otorgaron como consecuencia de dichos ardides hasta tanto se resuelva la acción principal o por un tiempo determinado (39).

La plataforma fáctica de estos casos en general se repite y el cliente del banco es víctima de un ardid o engaño mediante el mecanismo de phishing o vishing. Por esta vía extraños logran acceder a sus cuentas bancarias y contratar un préstamo personal, para luego transferir las sumas a cuentas de terceras personas.

En un caso de estas características llevado a los tribunales se hizo lugar a la medida cautelar innovativa ordenando al banco que se abstenga de efectuar los descuentos por el crédito que se había tomado afirmándose que "se debe velar por la prevención y cesación del daño; independientemente de los reclamos que las partes puedan formular en otros procesos de conocimiento; con la finalidad de acordar una tutela eficaz, preventiva y provisoria sobre el consumidor (usuario) mientras se investiga y esclarece lo ocurrido. Se procura intervenir preventivamente y mantener el estado actual hasta que se dilucide la cuestión" (40). En otro precedente (41) se confirmó la medida cautelar otorgada en primera instancia haciendo hincapié en la prevención del daño y afirmándose que "en cuanto al requisito del peligro en la demora, el mismo se aprecia razonablemente evidenciado a tenor de las sumas que aparecen involucradas en las operaciones crediticias cuya ineficacia se persigue y su trascendencia económica, lo cual permite inferir el consecuente daño inminente ante la vulnerabilidad económica que trae aparejado la continuidad del descuento de cuotas del préstamo". Además, se postuló que "es deber de la judicatura el evitar la consumación de un daño mayor, en una operatoria amparada por una legislación de orden público, tal la ley 24.240".

En similar sentido, se otorgaron medidas cautelares innovativas tendiente a que el banco demandado se abstenga de efectuar los descuentos del crédito otorgado ponderando que "la cautelar es la única vía apta para tutelar preventivamente el derecho invocado. El marco consumeril que rodearía la cuestión, impone adoptar aquellas medidas que procuren la salvaguarda del accionante, sin perjuicio de lo que en definitiva se resuelva" (42).

Por último, es necesario señalar que cuando existe una conducta desaprensiva de la entidad bancaria que implique un grave menosprecio de los derechos del consumidor resulta procedente la aplicación de daños punitivos no solo con fin sancionatorio sino para disuadir o prevenir conductas similares por la propia entidad u otras entidades bancarias. A esos fines se ponderó la conducta reiterada disvaliosa de la demandada al indicar la existencia de un precedente en otra Sala del mismo Tribunal que también la involucraba y en la que se advierte cierta identidad en la actuación desplegada. Dicha conducta reiterada configura el agravamiento necesario para tener por configurado el daño punitivo reclamado (43).

IV.2. Tutela resarcitoria

Una de las acciones que suelen entablarse frente a casos de phishing o vishing es la de daños y perjuicios contra la entidad bancaria vinculada contractualmente con el consumidor o usuario estafado. Ello sin perjuicio que, en algunos casos en que se haya podido individualizar al estafador, también se inicien acciones contra él. En este punto nos circunscribiremos a las acciones que se entablan contra el banco en —la mayoría de las veces en el marco de una relación de consumo—, y para ello analizaremos los cuatro presupuestos de responsabilidad de civil.

IV.2.a. Antijuridicidad

Como se puso de manifiesto en el punto III —al cual remitimos— existe una obligación de seguridad que pesa sobre el banco que tiene fundamento legal —arts. 5º y 6°, LDC— y constitucional —art. 42, CN— y que se encuentra reforzada por toda la normativa emitida por el BCRA en ese sentido.

Además, para cada caso concreto de phishing o vishing podrán existir otras conductas antijurídicas por parte

de la entidad bancaria, por ejemplo, el incumplimiento al deber de otorgamiento de préstamos responsablemente que surge implícita del art. 1387 del Cód. Civ. y Com. La entidad incumple esta obligación si otorga préstamos pre acordados en el marco de las estafas que se analizan, ya que incumple en forma flagrante la obligación de proveer la información que exige la norma.

IV.2.b. Factor de atribución

IV.2.b.i. Vicio o riesgo de la cosa o de la prestación del servicio, actividad riesgosa o garantía

El art. 1757 del Cód. Civ. y Com. establece que "toda persona responde por el daño causado por el riesgo o vicio de las cosas, o de las actividades que sean riesgosas o peligrosas por su naturaleza, por los medios empleados o por las circunstancias de su realización. La responsabilidad es objetiva. No son eximentes la autorización administrativa para el uso de la cosa o la realización de la actividad, ni el cumplimiento de las técnicas de prevención". Por su parte, el art. 1758 dispone que "el dueño y el guardián son responsables concurrentes del daño causado por las cosas. Se considera guardián a quien ejerce, por sí o por terceros, el uso, la dirección y el control de la cosa, o a quien obtiene un provecho de ella...", que en el caso que nos ocupa resulta ser la entidad bancaria.

Al respecto cabe recordar que, en el marco unificado de la responsabilidad civil, ningún impedimento existe para aplicar directamente a los daños sufridos por el acreedor con motivo u ocasión de la ejecución del contrato —con exclusión de los derivados del incumplimiento de los deberes de prestación— las normas que estructuran la responsabilidad extracontractual, y en particular las que se refieren a la responsabilidad por riesgo. Por consiguiente, si el deudor ha dañado al acreedor mediante el empleo de una cosa riesgosa o viciosa, o una actividad peligrosa, se aplicarán los arts. 1757 y 1758 del Cód. Civ. y Com. y aquel responderá objetivamente (44).

Como lo ha sostenido la jurisprudencia (45) anterior a la sanción del Cód. Civ. y Com. el sistema informático —software y hardware— puede ser calificado como una cosa riesgosa. De este modo, se ha considerado que el "sistema informático" es un conjunto de elementos materiales (hardware: servidores, cableado de datos y electricidad, cajeros automáticos, tarjetas magnéticas, etc.) que califican como cosa aun desde una interpretación restrictiva de tal concepto. Estos elementos "físicos" son complementados por otros elementos digitales (software), que contienen las instrucciones para que aquellos medios mecánicos o electrónicos cumplan las tareas para las cuales han sido diseñados.

Esta calificación fue asignada al sistema informático que opera las transacciones remotas, sea mediante el denominado homebanking sea por el uso de cajeros automáticos. En el precedente "Bieniauskas" se postuló que "un sistema informático en actividad que permite realizar pagos y extracciones de fondos de una cuenta bancaria y que opera de forma remota es naturalmente una cosa riesgosa. El riesgo se evidencia tanto para el usuario como para el Banco quien, por las propias características de su actividad, está expuesto a eventuales ataques de terceros". De hecho, en el caso de mención se puso de resalto que "la fragilidad del sistema quedó demostrada por el número de fraudes que, en un escaso tiempo, pudieron ser concretados mediante idéntica operatoria delictual".

Luego de la sanción del Cód. Civ. y Com., que incorpora las actividades riesgosas, no es necesario efectuar esfuerzos interpretativos. Tal como lo establece el art. 1757 las actividades pueden ser riesgosas por su naturaleza, por los medios empleados o por las circunstancias de su realización. Las actividades riesgosas por su naturaleza son aquellas que conforme al curso normal y ordinario de las cosas resultan intrínsecamente peligrosas por sí mismas, cualesquiera sean las circunstancias bajo las cuales se realizan (46). La actividad es riesgosa o peligrosa por los medios empleados cuando normalmente es inocua, pero adquiere aquella cualidad porque una persona hace uso de mecanismos, instrumentos, aparatos o sustancias que son peligrosas por la velocidad que desarrollan, por su naturaleza explosiva o inflamable, por la energía que contienen, por el lugar anómalo en que se encuentran o por otras causas análogas, o bien si han sido los medios utilizados los que han aumentado la probabilidad de riesgo (47). La actividad es peligrosa (por las circunstancias de su realización), cuando no obstante no revestir un peligro regular o constante, las modalidades de tiempo, modo y lugar la tornan peligrosa (48). En la actividad bancaria, las operaciones realizadas por medio de la tecnología constituyen actividades riesgosas, por los medios empleados (49).

En un precedente (50) se postuló que el sistema de homebanking puede ser calificado como cosa riesgosa, aunque estando en el ámbito contractual también puede resultar fundamento atributivo de responsabilidad el deber de garantía derivado de la obligación de seguridad de configuración objetiva. Tal garantía está preceptuada por normativa emanada del BCRA, en tanto estatuye que en "todos los casos, las entidades deberán tener implementados mecanismos de seguridad informática que garanticen la genuinidad de las operaciones". Lo que se debate es la seguridad (o vulnerabilidad) de un sistema automatizado que se utiliza a los fines de la

consecución del contrato habido entre las partes. De este modo, los clientes del banco verosímilmente pueden entender que el banco se comprometió a garantizar la seguridad del sistema de homebanking siendo esta una obligación de resultado.

Por último, debe tenerse presente que cuando resulte aplicable el estatuto consumeril, el art. 40 de la LDC establece una solución similar al Cód. Civ. y Com. fundado en un factor de atribución de responsabilidad objetivo al disponer que "si el daño al consumidor resulta del vicio o riesgo de la cosa o de la prestación del servicio, responderán el productor, el fabricante, el importador, el distribuidor, el proveedor, el vendedor y quien haya puesto su marca en la cosa o servicio... Solo se liberará total o parcialmente quien demuestre que la causa del daño le ha sido ajena".

Por su parte, el art. 10 bis de la LDC proclama la responsabilidad objetiva de los proveedores al estatuir como única causal liberatoria al caso fortuito o fuerza mayor, tornando al universo de obligaciones a su cargo en obligaciones de resultado —ello, con prescindencia de las circunstancias de cada obligación (51).

IV.2.b.ii. Juego de las eximentes en la actividad bancaria realizada a través de tecnología

En definitiva, al tratarse de un factor de atribución de responsabilidad objetivo —riesgo o vicios de la cosa o prestación del servicio, actividad riesgosa o garantía—, la entidad bancaria solo se libera demostrando la causa ajena (art. 1722 del Cód. Civ. y Com.), es decir, el hecho del damnificado o de la víctima (art. 1729 del Cód. Civ. y Com.), el hecho del tercero por quien no se debe responder (art. 1731 del Cód. Civ. y Com.) o el caso fortuito o fuerza mayor (art. 1730 del Cód. Civ. y Com.).

En los casos que analizamos, generalmente, las entidades bancarias demandadas plantean como eximente de su responsabilidad el hecho de la víctima por haber proporcionado al ciber delincuente datos que permitieron el acceso a sus cuentas o el hecho de terceros —los estafadores que realizan el hecho delictivo—, por quien no se debe responder.

Siguiendo a Pizarro (52), podemos afirmar que, para funcionar como eximente, "el hecho de la víctima debe, necesariamente, ser causa adecuada y exclusiva del daño o concausa del mismo, en concurrencia con otros factores relevan-tes". El autor cita a Kemelmajer de Carlucci para indicar que "ninguna influencia tiene la conducta del sindicado como responsable 'si no ha sido la causa adecuada del perjuicio' en forma exclusiva o concurrente. Cuando esto último sucede, el hecho de la víctima asume el carácter de una mera circunstancia, irrelevante para la producción del resultado final, por lo que carece de toda virtualidad eximitoria". Así, "el hecho de la víctima no debe ser imputable al demandado, objetiva o subjetivamente. Cuando este último es quien lo provoca, la acción de la víctima se presenta como una 'mera consecuencia del acto del ofensor' y resulta inapta para liberar al sindicado como responsable. Como consecuencia de lo dicho, la no adopción de medidas apropiadas para evitar que el daño se produzca pasa a ser una circunstancia determinante para que se produzca el hecho de la víctima" (53).

Esta cuestión asume singular importancia en la materia que tratamos. Por un lado, es evidente que la conducta del banco y la del cliente no pueden juzgarse con la misma vara (54). El primero es un profesional que diseña el sistema e impone su uso: se espera la máxima profesionalidad (art. 1725, Cód. Civ. y Com.). Por el otro, la conducta del consumidor tendrá que analizarse teniendo en cuenta la confianza que genera ese sistema predispuesto y sus escasas posibilidades de discernir si está interactuando con un representante del banco o con un impostor.

Desde el punto de vista causal, consideramos que existen dos instancias fundamentales en las que los bancos podrían evitar el daño: en la verificación de la identidad del usuario en el ingreso y en la verificación de su intención ante la realización de determinados actos. De ese modo, la eximente "culpa de la víctima" no puede funcionar.

Las entidades bancarias podrían evitar el daño utilizando sistemas más confiables para verificar la identidad del usuario. De hecho, el elegido es el más inseguro de los existentes. Pensemos que basta con que el consumidor engañado brinde un par de datos para que alguien se apodere de sus cuentas y actúe como el más facultado de los mandatarios. Si se adoptaran métodos más seguros, ese hecho carecería de virtualidad para permitir que el impostor se apoderara de la cuenta, pues se le exigirían otros elementos de verificación. Causalmente, entonces, la conducta de la víctima no es la que permite el daño como venimos afirmando.

Otra de las eximentes que suele ser invocada es el hecho del tercero por quien no se debe responder, que. para eximir total o parcialmente de responsabilidad, debe reunir los caracteres del caso fortuito (art. 1731). En tal sentido, se considera caso fortuito o fuerza mayor al hecho que no ha podido ser previsto o que, habiendo sido previsto, no ha podido ser evitado (art. 1730). Por lo demás, "aunque ocurra el caso fortuito..., el deudor es responsable ... e) Si el caso fortuito ... constituye una contingencia propia del riesgo de la cosa o de la actividad" (art. 1733 del Cód. Civ. y Com.).

Se ha sostenido con acierto que el robo o hurto de un local bancario, hipótesis que se extiende a un cajero automático es un hecho previsible y por tanto objeto de resguardos por el banco. La normativa del BCRA no solo brinda instrucciones a los bancos en materia de seguridad en sus locales sino también en lo relativo a las transacciones electrónicas. Así mal puede sostenerse que este hecho no pudiera ser previsto por el banco. En rigor, debe ser objeto de particular atención por la entidad bancaria en orden a ofrecer a sus clientes la suficiente seguridad para evitar los previsibles y reiterados ataques de delincuentes. Las agresiones pueden concretarse mediante ataques físicos como electrónicos. Al no hacerlo, o fallar en el intento, el hecho de estos terceros no permite eximir al banco de su clara responsabilidad (55).

Asimismo, en otro caso jurisprudencial se arribó a una conclusión similar al postularse que la conducta de aquellos que habrían violado la integridad del sistema informático carece de aptitud para liberar la responsabilidad de la accionada, en tanto constituye un hecho previsible y, por ello, objeto de resguardo por parte de cualquier entidad bancaria (56).

IV.2.c. Daño indemnizable

El daño patrimonial o económico importa, necesariamente, un detrimento del patrimonio de la persona, como conjunto de valores económicos, susceptible de apreciación pecuniaria, para lo cual deben tomarse en consideración todas las circunstancias del caso concreto. El daño patrimonial produce una merma en el patrimonio del damnificado y su indemnización, en términos de razonable equivalencia, luce orientada a recomponerlo (57).

En este tipo de maniobras, en general, el daño patrimonial estará dado por los montos que hayan sido objeto de la extracción fraudulenta de las cuentas del cliente del banco como, así también, por las sumas que haya tenido que abonar en concepto de préstamo bancario otorgado sin su consentimiento.

Por su parte, el daño extrapatrimonial o moral es una minoración en la subjetividad de la persona humana, derivada de la lesión a un interés no patrimonial. O, con mayor precisión, una modificación disvaliosa del espíritu, en el desenvolvimiento de su capacidad de entender, querer o sentir, consecuencia de una lesión a un interés no patrimonial, que habrá de traducirse en un modo de estar diferente de aquel al que se hallaba antes del hecho, como consecuencia de este y anímicamente perjudicial (58).

En el precedente "Bieniauskas" (59) se hizo lugar a la demanda de daño material y moral en su integridad tanto en la sentencia de primera instancia como en la Cámara que la confirmó. En otro fallo (60) se revocó la sentencia de primera instancia que había rechazado la demanda y en su lugar se hizo lugar al daño patrimonial reclamado constituido por tres transferencias que se habían efectuado sin autorización del titular de la cuenta.

Como es evidente, ser objeto de una ciber estafa de la naturaleza de las que estamos analizando y que impliquen no solo el vaciamiento de las cuentas —muchas veces con todos los ahorros de la persona—, sino también que se otorguen prestamos no consentidos cuyos montos deben ser reintegrados al banco con intereses, genera una minoración espiritual de gran trascendencia. No se trata de meras molestias sino de angustias que deben ser adecuadamente resarcidas.

En este sentido, se ha valorado para el otorgamiento del resarcimiento del daño no patrimonial la incomprensión por parte del banco con quien se operaba normalmente y la imputación de que dichas operaciones fueron realizadas por el cliente y/o por su torpeza al brindar sus claves personales a terceros (61).

Asimismo, se sostuvo que, en algunas oportunidades, el daño moral no requiere de una prueba acabada, sino que es admisible inferirlo razonablemente de las circunstancias. Fue el caso en el que se consideró que era indudable que la usuaria había sufrió un menoscabo espiritual al verse privada de los salarios que tenía depositados en su cuenta mediante una maniobra fraudulenta que el banco conocía y había denunciado ante la Justicia y frente a la cual permaneció inactivo omitiendo alertar debidamente a sus clientes (62).

Asimismo, en otro precedente se admitió el rubro daño moral también valorándose el comportamiento del banco demandado ya que luego de conocido el ilícito no atendió su deber de respetar la dignidad del consumidor dando respuesta adecuada al usuario defraudado mostrándose insensible al respecto. Se postuló que, si bien la actora sufrió una triste experiencia, la indemnización le ha de poder otorgar satisfacciones sustitutivas para aliviar u olvidar el sinsabor experimentado (63).

IV.2.d. Relación de causalidad

La relación de causalidad es la necesaria conexión fáctica que debe existir entre la acción humana y el resultado dañoso producido. En el ámbito contractual y de la relación de consumo, la relación de causalidad vincula materialmente, de manera directa, el incumplimiento con el daño y, en forma sucedánea e indirecta, a este con el factor de atribución. Se trata de resolver si un resultado dañoso determinado puede ser materialmente atribuido a una persona física o jurídica (64).

En esta línea, el art. 1726 del Cód. Civ. y Com. dispone que "son reparables las consecuencias dañosas que tienen nexo adecuado de causalidad con el hecho productor del daño. Excepto disposición legal en contrario, se indemnizan las consecuencias inmediatas y las mediatas previsibles". Son consecuencias inmediatas aquellas que acostumbran a suceder, según el curso normal y ordinario de las cosas (art. 1727, Cód. Civ. y Com.). La inmediatez no deriva de la cercanía temporal o espacial con el hecho generador; asume tal carácter porque entre el hecho generador y la consecuencia no se advierte la presencia de ningún hecho intermedio. La previsibilidad está siempre implícita en ellas, pues conforme al principio de regularidad siguen de manera natural y ordinaria a un hecho, situación que determina su necesaria representación en la mente de un hombre normal (65). Con relación a lo dicho el art. 1728 del Cód. Civ. y Com. dispone: "En los contratos se responde por las consecuencias que las partes previeron o pudieron haber previsto al momento de su celebración...".

Se ha afirmado que todos los elementos que revelan una reingeniería en la prestación de los servicios bancarios y un incipiente pero constante cambio cultural hacia el uso de medios informáticos, son trascendentes para interpretar la conducta de las partes y la responsabilidad que sigue frente a un hecho irregular como el aquí analizado. Cabe reparar que el banco debe procurar como mínimo, brindar igual seguridad que si tal operatoria se realizara personalmente. Esa seguridad no está dada prioritariamente por el local donde el usuario interactúa con el cajero automático o la custodia policial del lugar sino esencialmente por la confianza que brinda el medio empleado. Confianza que, por ejemplo, no solo radica en el uso de una clave personal y única, sino también por la esperable inviolabilidad de la tarjeta magnética entregada como del software utilizado por el banco (66).

Por último, a los fines de valorar la conducta de la entidad bancaria no se puede dejar de considerar su calidad de experto o profesional con relación al cliente del banco (art. 1725). En esta línea se ha sostenido que las entidades financieras deben adoptar mayores recaudos habida cuenta de su condición de profesional debido a la obligación que asumen y la actividad que desarrollan, por ello debe apreciarse su conducta con un standard de responsabilidad agravada (67).

En otras palabras, existe una relación de superioridad entre el experto y el profano que no puede ser soslayada. Esta superioridad se derrama en las relaciones contractuales tanto en lo relativo a su faz jurídica —contratos predispuestos— como a la especialidad técnica. Así, son las entidades bancarias quienes se encuentran en una posición ventajosa frente al usuario en tanto ostentan la información y todas las aptitudes técnicas para ofrecer seguridad y en su caso, brindar la prueba que otorgue al juez un cabal conocimiento de lo ocurrido (68). Por otro lado, se encuentran autorizadas por el Estado para tomar los ahorros públicos, lo cual les exige un mayor cuidado en su actividad y un particular celo en el cuidado de los bienes que le son puestos a su cuidado.

Y en casos como los analizados en que la ejecución prestacional presenta riesgos, la obligación de seguridad cumple un rol crucial ya que permite modular si el deudor ha cumplido con los estándares de seguridad que diligentemente las circunstancias del caso le imponían (arts. 1725 del Cód. Civ. y Com.) (69).

En definitiva, cuanto más compleja sea la actividad empresarial más aumenta la obligación de sus organizadores de prever las consecuencias posibles de los hechos debiendo asegurar un correcto cumplimiento de la prestación a su cargo.

IV.3. Pretensión declarativa de nulidad de los créditos

Como se puso de manifiesto en los puntos precedentes, en general en las maniobras delictivas de phishing o vishing se suelen tomar créditos sin el consentimiento del titular de la cuenta bancaria vulnerada. Esta situación ha generado que se entablen acciones judiciales tendientes a que se declare la nulidad de esos mutuos.

Es decir, los préstamos que se cuestionan constituyen actos jurídicos celebrados con una voluntad viciada por dolo en el elemento intención. De este modo, el art. 271 establece que "acción dolosa es toda aserción de lo que es falso o disimulación de lo verdadero, cualquier artificio, astucia o maquinación que se emplee para la celebración del acto...". Por su parte, se trata de un supuesto de dolo esencial (art. 272 del Cód. Civ. y Com.) que causa la nulidad del acto. Ello es así, porque reúne las características de ser grave, determinante de la voluntad, que causa un daño importante y no existe dolo del cliente engañado. En los casos que se analizan, el dolo es ocasionado por un tercero —ciber delincuente— con relación al acto —préstamo otorgado—.

Más allá de resultar aplicable la normativa antes citada, cuando nos encontramos en el ámbito de aplicación de las normas tuitivas consumeriles se puede arribar a la nulidad del acto invocando otra normativa. El art. 37 in fine de la LDC dispone que "en caso en que el oferente viole el deber de buena fe en la etapa previa a la conclusión del contrato o en su celebración o transgreda el deber de información..., el consumidor tendrá derecho a demandar la nulidad del contrato o la de una o más cláusulas...". En estos casos, en los que se ve francamente violentado el deber de buena fe y la obligación de informar, la norma presume la existencia de un vicio del consentimiento y habilita solicitar la nulidad del acto.

Por último, el art. 1389 del Cód. Civ. y Com. emplazado en la regulación de los contratos bancarios con usuarios y consumidores preceptúa que "son nulos los contratos de crédito que no contienen información relativa al tipo y partes del contrato, el importe total de financiamiento, el costo financiero total y las condiciones de desembolso y reembolso". Independientemente de la maniobra engañosa que lleva al otorgamiento del crédito, en muchos casos la información que exige la norma no es proporcionada por la entidad bancaria tornando nulo el contrato de crédito por dicho motivo.

En esta línea, se declaró la nulidad del préstamo otorgado en un caso en que la actora al ir a retirar dinero del cajero automático fue guiada por una agente municipal quien permaneció a su lado mientras efectuaba la extracción y luego mediante un ardid logró cambiar el plástico entregándole la tarjeta de un tercero y con su tarjeta tomó un préstamo y extrajo luego el dinero. La inspectora municipal resultó condenada penalmente. En la sentencia civil se sostuvo que estamos frente a un supuesto de absoluta ineficacia por nulidad, pues la tecnología posibilitó la existencia de un negocio sin que haya intervenido la voluntad de la obligada y, en consecuencia, el banco no puede requerir el cumplimiento de ninguna contraprestación a la titular de la cuenta. Se trató de un delito perpetrado contra la entidad bancaria y no una operación ordinaria de ATM. El argumento fundante fue la confianza suscitada en los usuarios ya que estos confían en que el sistema bancario está rodeado de precauciones para evitar incidencias indeseadas y que todo está organizado para el correcto funcionamiento del servicio (70).

En otro precedente el planteo se efectúo a través de una acción mere declarativa y el juzgador la recondujo en una acción de nulidad (71).

V. Conclusión

Existen innumerables beneficios que nos proporciona la revolución digital y tecnológica. Como contracara se nos presentan diversas problemáticas en las que la tecnología incrementa la vulnerabilidad de los consumidores, tornando absolutamente necesaria su tutela. Entre las problemáticas que surgieron en la realidad social nos encontramos con nuevos tipos de fraudes tecnológicos o ciber estafas basados en la ingeniería social como el phishing o vishing.

Los conflictos que se susciten como consecuencia de estos deben ser analizados desde el prisma de la obligación de seguridad que pesa sobre la entidad bancaria y que constituye una obligación de resultado en cuanto debe brindar al cliente una prestación funcional preparada para hacer frente a previsibles maniobras fraudulentas de terceros. En este sentido, al haberse sustituido el sistema de atención "humana" por el "automático", la entidad debe otorgar al cliente la misma seguridad que existe cuando la operación se hubiera hecho a través del primero.

Es el banco el que tiene el deber de tomar medidas adecuadas de seguridad, para prevenir y evitar el hecho delictivo. Por ello, la obligación de seguridad impone a la entidad bancaria arbitrar todos los medios para evitar que el riesgo inherente al sistema se concrete en un daño para sus clientes.

Así, la entidad bancaria debería, además, de proporcionar credenciales de acceso y un segundo factor de autenticación (token), implementar sistemas más robustos de verificación de identidad, alertas de seguridad y sistemas de detección que permitan verificar si se accede a la cuenta desde un dispositivo diferente o si se realizan operaciones que no corresponden con el perfil del cliente, como la obtención de un crédito por canales electrónicos y su inmediata transferencia a cuentas que ni siquiera tiene vinculadas. Asimismo, el banco no puede permitir el otorgamiento, en forma inmediata, un crédito (72).

Dentro de las herramientas procesales y de fondo que nos proporciona nuestro ordenamiento jurídico para dar respuesta satisfactoria a esta problemática encontramos acciones judiciales que tienen por finalidad prevenir o evitar el agravamiento de los daños ya irrogados; en otros supuestos tienen por objeto la reparación de los daños y perjuicios ocasionados e incluso, algunas pretensiones tienden a sancionar conductas de la entidad bancaria que denotan un grave menosprecio a los derechos del consumidor o usuario de servicios financieros. Por último, existen acciones que tienden a declarar la nulidad de los créditos otorgados sin consentimiento del cliente del banco.

El factor atributivo de responsabilidad es de carácter objetivo fundado ya sea en la obligación de seguridad o el carácter de actividad riesgosa de los medios empleados. Por ello, el banco solo se liberará demostrando la causa ajena (art. 1722 del Cód. Civ. y Com.), es decir, el hecho del damnificado o de la víctima (art. 1729 del Cód. Civ. y Com.), el hecho del tercero por quien no se debe responder (art. 1731 del Cód. Civ. y Com.) o el caso fortuito o fuerza mayor (art. 1730 del Cód. Civ. y Com.), en la medida en que cumplan con todos los requisitos legales.

Con relación al juego de las eximentes de responsabilidad existen dos instancias fundamentales en las que

los bancos podrían evitar el daño: en la verificación de la identidad del usuario en el ingreso y en la verificación de su intención ante la realización de determinados actos. Si se adoptaran métodos más seguros, el hecho que la víctima engañada proporcione las claves de acceso carecería de virtualidad para permitir que el impostor se apoderara de la cuenta, pues se le exigirían otros elementos de verificación. De ese modo, la eximente "culpa de la víctima" no puede funcionar.

Por último, para que opere la eximente del hecho del tercero por quien no se debe responder, debe reunir los caracteres del caso fortuito. Los hechos relatados son conocidos y previsibles y por tanto deberían ser objeto de resguardos por el banco. En otras palabras, la entidad bancaria debe ofrecer a sus clientes la suficiente seguridad para evitarlos.

(*) Profesora adjunta de Derecho de los Contratos y de Derecho del Consumidor de la Facultad de Derecho de la Universidad Nacional de Rosario, presidenta del Instituto de Protección Jurídica del Consumidor del Colegio de Abogados de Rosario, miembro del Instituto Argentino de Derecho del Consumidor, magíster en Derecho Privado graduada en la Facultad de Derecho de la Universidad Nacional de Rosario, doctoranda en Derecho en la Facultad de Derecho de la Universidad Nacional de Rosario, investigadora categoría 3 en el marco del Programa de Incentivos a docentes investigadores, abogada litigante en el ejercicio independiente de la profesión.

(**) Abogado, egresado de la Facultad de Derecho, Universidad Nacional de Mar del Plata. Secretario letrado ante la Cámara Federal de Apelaciones de Mar del Plata. Docente en la materia Derecho Penal - Parte Especial, Facultad de Derecho, Universidad Nacional de Mar del Plata.

(1) En abril de 2020 la facturación por venta online creció un 84% en comparación con el promedio del primer trimestre del año (https://www.cace.org.ar/noticias-el-comercio-electronico-crecio-84-en-abril#:~:text=NOVEDADES.&text=El%20comercio%20e

(2) LORENZETTI, Ricardo L., "Comercio electrónico", Ed. Abeledo-Perrot, Buenos Aires, 2001, p. 218.

(3) Véase https://www.infobae.com/tendencias/talento-y-liderazgo/2020/02/11/era-digital-quienes-son-losanalfabetos-del-siglo-xxi/.

(4) LORENZETTI, Ricardo L., "Comercio electrónico", ob. cit., p. 49.

(5) LORENZETTI, Ricardo L., "Comercio electrónico", ob. cit., p. 221.

(6) TAMBUSSI, Carlos E., "Relación de consumo y responsabilidad objetiva entre los usuarios de plataformas de venta y el proveedor del servicio", LA LEY, 2018-C, 101; RCyS 2018-VII, 59; AR/DOC/789/2018.

(7) WAJNTRAUB, Javier H., "Los consumidores con vulnerabilidad agravada en la reciente normativa", LA LEY, 2020-C, 815.

(8) SAHIÁN, José H., "El principio antidiscriminatorio en la relación de consumo", SJA del 18/09/2019; AR/DOC/2635/2019.

(9) CHAMATRÓPULOS, Demetrio A., "Estatuto del consumidor comentado", Ed. La Ley, Buenos Aires, 2019, 2ª ed., t. I, p. 165.

(10) ÁLVAREZ LARRONDO, Federico M., "Desafíos para el derecho en general, y del consumo en particular. La construcción del nuevo 'derecho artificial' y la excusa para cambiar el rumbo de la Argentina", RDCO 292-119, 01/11/2018; AP/DOC/729/2018.

(11) JCiv. y Com. N.º 10 de La Plata, 27/08/2020, "Pedernera, Juan Alberto c. Banco de la Provincia de Buenos Aires s/ acción declarativa (trám. sumarísimo)", LLOnline AR/JUR/34631/2020.

(12) https://www.infotechnology.com/mundo-cio/el-ano-de-los-ciberataques-como-hicieron-los-bancos-argentinos-para-defender-a-sus

(13) https://defensoria.org.ar/noticias/phishing-encuen-tro-con-asociaciones-bancarias/, https://www.eldiariosur.com/provinciales/2021/3/8/estafas-clientes-del-banco-bbva-frances-crecen-los-casos-45505.html. https://www.eldiariosur.com/esteban-echeverria/2020/11/9/estafas-clientes-del-bbva-frances-la-mirada-de-los-expertos-43678.htm y https://www.eldiariosur.com/provinciales/2021/3/8/estafas-clientes-del-banco-bbva-frances-crecen-los-casos-45505.html.

(14) www.oecd.org/finance/Financial-Consumer-Protection-Policy-Approaches-in-the-Digital-Age.pdf.

(15) https://www.perfil.com/noticias/tecnologia/ciberdelincuencia-denuncias-por-estafas-bancarias-aumentaron-3-mil-por-ciento-en-pa

(16) https://www.cronista.com/finanzas-mercados/bancos-cerraron-214-sucursales-en-los-primeros-seis-meses-de-cuarentena/.

(17) La capacidad del usuario de controlar por sí mismo se ve muy limitada por algunas características de la red. Los procesos de identificación en el mundo real son diferentes de los que acostumbramos a utilizar: si uno entra en una tienda, existen exigencias municipales que regulan su apertura, marcas registradas, elementos físicos, lo que da una cierta seguridad. En Internet uno se pregunta: ¿lo que se presenta como un banco, lo es en verdad?; la página que dice ser de una compañía de turismo, ¿pertenece realmente a ella? La red diluye la potencialidad de los procesos de identificación y autoría (LORENZETTI, Ricardo L., "Comercio electrónico", ob. cit., p. 24).

(18) https://www.baenegocios.com/negocios/Banco-Galicia-se-va-de-Instagram-por-las-estafas-virtuales-20200911-0103.html: "No solo se contactan a través de llamados telefónicos, mensajes de WhatsApp o contactando a gente mayor para decirle que pasarán a buscar sus billetes porque saldrán de circulación, aparecen donde menos se los espera. Desde que empezó la pandemia comenzaron a utilizar cada vez más las redes sociales y en especial Instagram. Una red que uno imagina que tiene usuarios que jamás podrían caer en un engaño, porque son más jóvenes, conocen la cultura digital, son "más despiertos". Grave error. En las últimas horas, el Banco de Galicia tuvo que hacer una dura decisión y la comunicó en sus redes: "A partir del 16 de septiembre cerramos Instagram por un tiempo. Si te contactan por acá no somos nosotros. Desde nuestros canales reforzamos los mensajes de alerta por estafas virtuales. Pero sabemos que es difícil diferenciar las comunicaciones falsas de las oficiales. Por eso decidimos irnos temporalmente de la red social donde ocurren las estafas".

(19) CS, Fallos 329:646, 21/03/2006, "Ferreyra, Víctor D. y Ferreyra, Ramón c. VICOV SA s/ daños y perjuicios", consid. 6º.

(20) GHERSI, Carlos, "Responsabilidad de las Entidades Bancarias", Ed. Universidad, p. 40.

(21) BARBIER, Eduardo A., "Contratación bancaria", Ed. Astrea, 2008, 3ª ed. act. y amp., t. 1, Consumidores y Usuarios, p. 337.

(22) CHAMATRÓPULOS, Demetrio A., "El deber de seguridad de los bancos y los daños derivados de la utilización de cajeros automáticos", RCyS 2010-IX, 95.

(23) CNCom., sala C, 22/12/2009, "De Santis, Ulises M. y otro c. Banco de la Ciudad de Buenos Aires". En primera instancia se había considerado que existió culpa de la víctima pues se había difundió el PIN a terceros, ignorando las advertencias de seguridad realizadas por el Banco a tal efecto. La Cámara revoca dicha resolución.

(24) CNCom., sala D, 11/08/2009, "Zappettini, Raúl M. c. Banelco SA", JA 70054894, LLOnline 20090796.

(25) RITTO, Graciela, "Acerca de la responsabilidad de los bancos por el correcto funcionamiento de los cajeros automáticos", RCyS 2010-II, 210 comentando el fallo CCiv. y Com. Junín, 15/10/2009, "Barni, Mauricio O. c. Banco Río de La Plata SA y otro".

(26) Comunicación "A" 6878, arts. 1.6.2, 1.6.3, 1.7.2, 1.7.3 y 3.4.5.

(27) JCiv. y Com. Común VI de Tucumán, 04/12/2020, "Nassif Oubeid de Caucota, Paola A. y otro c. Banco Macro SA s/ sumarísimo (residual)" (expte. 2695/20).

(28) LÓPEZ MEZA — TRIGO REPRESAS, "Tratado de la responsabilidad civil", 2ª ed. act., t. II, p. 829.

(29) https://www.infotechnology.com/mundo-cio/el-ano-de-los-ciberataques-como-hicieron-los-bancos-argentinos-para-defender-a-sus

(30) PIZARRO, Ramón D., "Responsabilidad civil por riesgo creado y de empresa", LA LEY, 2006-I, p. 266.

(31) LÓPEZ MEZA — TRIGO REPRESAS, "Tratado...", ob. cit., t. II, p. 832.

(32) GOLDEMBERG, Isidoro, "La relación de causalidad en la responsabilidad civil", Ed. La Ley, 2000, 2ª ed., p. 150.

(33) CCiv. y Com. de Rosario, sala II, "Ronalb SRL c. Banco Macro SA s/ daños y perjuicios" (CUIJ 21-01482504-2), Acuerdo 6 del 05/02/2021.

(34) LORENZETTI, Ricardo L., "La tutela civil inhibitoria", LA LEY, 1995-C, 1217.

(35) GALDÓS, Jorge M., "El mandato preventivo una valiosa herramienta procesal de la responsabilidad

civil", Revista de Derecho de Daños, "Prevención del daño" 2016-2, Ed. Rubinzal Culzoni, Santa Fe, p. 347.

(36) GALDÓS, Jorge M., "La prevención del daño en las nuevas tecnologías. La tutela preventiva en las redes sociales", EBOOK-TR 2021 TOBÍAS, 21/01/2021, 126, LL AR/DOC/3462/2020.

(37) PIZARRO, Ramón D., "¿Réquiem para la obligación de seguridad en el Código Civil y Comercial?", LA LEY del 21/09/2015, 1; LA LEY, 2015-E, 840; LL AR/DOC/2538/2015.

(38) Se la puede considerar de "no innovar", en el sentido de impedir que se comiencen a efectuar descuentos o "innovativa" para que se suspendan los que puedan haberse dispuesto por la entidad bancaria. En el caso de la medida cautelar innovativa una vez dictada altera la situación de hecho o de derecho existente antes de su petición, y se traduce en la injerencia del juez en la esfera de los justiciables mediante la orden de que cese una actividad presuntamente contraria a derecho o de que se retrotraigan las consumadas de una actividad de tal tenor. Mediante esta medida se dispone una mutación del estado de hecho existente, lo que da razón a la orden judicial, de modificación anticipada de una situación jurídica.

(39) JCiv. y Com. 2da. Nom. de Villa Constitución, sep. 2020, "Bressan, Elvira R. c. BBVA Banco Francés s/ demanda de derecho de consumo"; CApels. de Bahía Blanca, 29/09/2021, "Palacios, María Claudia c. Santander Río SA s/ nulidad del acto; JNCom. N.º 14, 06/05/2021, "Ayala González, César A. c. Banco BBVA Argentina SA s/ ordinario" (expte 5237/2021).

(40) JCiv. y Com. N.º 1 de Pergamino, 21/09/2020, "Raggio, Alejandro c. Banco de la Provincia de Buenos Aires s/ medidas cautelares (traba/levantamiento)"; "Pedernera, Juan Alberto c. Banco de la Provincia de Buenos Aires s/ acción declarativa (trám. sumarísimo)", LL AR/JUR/34631/2020 y C. 2a Civ. y Com. La Plata, sala I, 05/11/2020, "Pedernera, Juan Alberto c. Banco de la Provincia de Buenos Aires s/ nulidad de acto jurídico (incidente art. 250 del Cód. Proc. Civ. y Com.)", LL AR/JUR/ 55654/2020.

(41) CNCom., sala F, 13/04/2021, "Gabrielich, Silvia E. c. Banco Santander Río SA s/ medida precautoria" (expte. 1191/2021).

(42) JCiv. y Com. Común VI de Tucumán, 04/12/2020, "Nassif Oubeid de Caucota, Paola A. y otro c. Banco Macro SA s/ sumarísimo (residual)" (expte. 2695/20) y Juz. en feria, 08/01/2021, "Abaca Diambra, Julieta c. BBVA Argentina SA s/ sumarísimo (residual)" (expte. 4244/20).

(43) CCiv. y Com. de Rosario, sala II, "Ronalb SRL c. Banco Macro SA s/ daños y perjuicios" (CUIJ 21-01482504-2), Acuerdo 6 del 05/02/2021.

(44) PICASSO, Sebastián, "Réquiem para la obligación de seguridad en el derecho común", RCCyC 2015 (julio), LL AR/DOC/2127/2015.

(45) CNCom., sala D, 15/05/2008, "Bieniauskas, Carlos c. Banco de la Ciudad de Buenos Aires", LA LEY del 21/07/2008, p. 3.

(46) PIZARRO, Ramón D., "Responsabilidad civil por actividades riesgosas o peligrosas en el nuevo código", LA LEY, 2015-D, 993, LL AR/DOC/2550/2015.

(47) GALDÓS, Jorge M., "Responsabilidad civil por actividades riesgosas y peligrosas en el nuevo código", LA LEY, 2016-B, 891, LL AR/DOC/751/2016.

(48) ENGHELMAYER, Fernando A., "Responsabilidad derivada de cierta actividades riesgosas o peligrosas en el Código Civil y Comercial de la Nacional", RCyS 2016-XII, 24, LL AR/DOC/2101/2016.

(49) DE NÚÑEZ, Rodrigo, "La responsabilidad objetiva en la actividad bancaria", SJA del 27/06/2018, p. 5; LL AR/DOC/3012/2018.

(50) CCiv. y Com. de Rosario, sala IV, 13/10/2017, "Red del Interior SRL c. Banco Macro SA s/ daños y perjuicios".

(51) DE NÚÑEZ, Rodrigo, "La responsabilidad...", ob. cit.

(52) PIZARRO, Ramón D., "Responsabilidad civil...", ob. cit., t. I, p. 245.

(53) PIZARRO, Ramón D., "Responsabilidad civil...", ob. cit., ps. 251 y ss.

(54) "El producto que está constituido por información es: - intangible, y por ello renuente a la comprobación empírica que el consumidor está acostumbrado a efectuar como prueba de fiabilidad: - hermético, en el sentido de que presenta una ajenidad respecto de la posibilidad de conocerlo sobre la base del grado de conocimiento que ya se tiene respecto de otros productos; cambiante y flexible y, por lo tanto, de poco sirve la experiencia anterior. Está inserto en un sistema de relaciones complejo, puesto que presenta múltiples interacciones con otros sujetos u otras partes. El producto es, entonces, un verdadero desafío para el consumidor". (LORENZETTI, Ricardo L., "Comercio electrónico", ob. cit., p. 221).

(55) CNCom. sala D, 15/05/2008, "Bieniauskas, Carlos c. Banco de la Ciudad de Buenos Aires", LA LEY del 21/07/2008, p. 3.

(56) CCiv. y Com. de Rosario, sala IV, 13/10/2017, "Red del Interior SRL c. Banco Macro SA s/ daños y perjuicios".

(57) PIZARRO - VALLESPINOS, "Tratado de Responsabilidad Civil", Ed. Rubinzal Culzoni, Santa Fe, 2017, t. I. Parte General, p. 134.

(58) PIZARRO - VALLESPINOS, "Tratado...", ob. cit., p. 138.

(59) CNCom. sala D, 15/05/2008, "Bieniauskas, Carlos c. Banco de la Ciudad de Buenos Aires", LA LEY del 21/07/2008, p. 3.

(60) CCiv. y Com. de Rosario, sala IV, 13/10/2017, "Red del Interior SRL c. Banco Macro SA s/ daños y perjuicios".

(61) JCiv. y Com. de Distrito de la 4ª Nom. de Rosario, "Gómez, Betsabé Martina c. Banco de Galicia y de Bs. As. SAU s/ demanda de derecho de consumo" (CUIJ 21-02934188-2), mayo 2021. No se encuentra firme.

(62) CNCom., sala E, 30/06/2008, "Traverso, María del Carmen c. Banco de la Ciudad de Buenos Aires", LL AR/JUR/8859/2008.

(63) JCiv. y Com. 1ª Nom. Reconquista, 03/03/2021, "Roda, Ramona L. c. Nuevo Banco de Santa Fe SA s/ demanda de derecho de consumo" (CUIJ 21-25024792-0).

(64) PIZARRO - VALLESPINOS, "Tratado...", ob. cit., p. 341.

(65) PIZARRO - VALLESPINOS, "Tratado...", ob. cit., ps. 373 y ss.

(66) CNCom. sala D, 15/05/2008, "Bieniauskas, Carlos c. Banco de la Ciudad de Buenos Aires", LA LEY del 21/07/2008, p. 3.

(67) JCiv. y Com. de Distrito de la 4ª Nom. de Rosario, "Gómez, Betsabé M. c. Banco de Galicia y de Buenos Aires SAU s/ demanda de derecho de consumo" (CUIJ 21-02934188-2), mayo 2021. No se encuentra firme.

(68) LÓPEZ MEZA — TRIGO REPRESAS, "Tratado...", ob. cit., Ed. La Ley, Buenos Aires, t. IV, p. 433.

(69) PIZARRO, Ramón D., "¿Réquiem...?", ob. cit.

(70) JCiv. y Com. 1ª Nom. Reconquista, 03/03/2021, "Roda, Ramona L. c. Nuevo Banco de Santa Fe SA s/ demanda de derecho de consumo" (CUIJ 21-25024792-0).

(71) JCiv. y Com. N.º 10 de La Plata, 27/08/2020, "Pedernera, Juan Alberto c. Banco de la Provincia de Buenos Aires s/ acción declarativa (trám. sumarísimo)", LL AR/JUR/34631/2020.

(72) AZZOLIN, Horacio —responsable de la Fiscalía General ante la Cámara Federal de Apelaciones de Bahía Blanca y titular de la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI)—, https://www.fiscales.gob.ar/ciberdelincuencia/piden-que-se-confirme-una-medida-cautelar-que-ordeno-al-banco-nacion-suspender-