

Responsabilidad de las entidades bancarias ante estafas electrónicas. El deber de seguridad y prevención en el marco del contrato de consumo

Responsibility of Banking Entities against Electronic Fraud. The Duty of Safety and Prevention within the Framework of the Consumer Contract

*María Paula Carril**

Resumen

Resulta necesario profundizar el análisis de la responsabilidad de las entidades bancarias ante la explosión de estafas electrónicas –que, sobre todo, proliferaron durante la pandemia–, cuyas víctimas resultaron ser –en su mayoría– los consumidores de servicios bancarios. En los tiempos de auge de nuevas y modernas tecnologías, es imperioso que las entidades bancarias intensifiquen los recaudos para una efectiva prevención y concientización ante ataques de ciberdelincuentes que constantemente modernizan los mecanismos de búsqueda y captación de datos, claves personales y contraseñas de sus clientes. La obligación de seguridad se desprende directamente del mandato constitucional contenido en el art. 42 de la Constitución Nacional, que enumera, entre los derechos básicos de los consumidores, “la protección de su seguridad e intereses económicos”. La modalidad más usual por la que se llevan a cabo las estafas electrónicas es la denominada *phising*, no obstante, existen otras que también son desarrolladas por ciberdelincuentes. En líneas generales, y ante la configuración del incumplimiento en lo que es materia propia del deber de prevención y seguridad que el ente bancario debe cumplir en el marco del contrato de consumo, el daño punitivo resulta enteramente procedente.

* Abogada por la Universidad Católica de Santiago del Estero. Posgrado en Derecho Laboral por la UBA, Posgrado en Derecho Penal y Diversidad Cultural por la UNJU. Secretaria de la Fiscalía General del Superior Tribunal de Justicia de la Provincia de Jujuy. Investigadora independiente. Contacto: mpcarril@justiciajujuy.gov.ar

Palabras clave: responsabilidad – estafas electrónicas – *phishing* – seguridad y prevención – daño punitivo

Abstract

It seems necessary to deepen the analysis of the responsibility of banking entities in the face of the explosion of electronic fraud –which, above all, proliferated during the pandemic–, whose victims turned out to be –mostly– consumers of banking services. In times of the rise of new and modern technologies, it is imperative that banking entities intensify precautions for effective prevention and awareness against attacks by cybercriminals who are constantly modernizing the mechanisms used for searching and capturing data, personal codes and passwords of their clients. The security obligation emanates directly from the constitutional mandate contained in article 42 of the National Constitution, which lists, among the basic rights of consumers, “the protection of their security and economic interests”. The most common modality by which electronic scams are carried out is called “phishing”, however, there are other modalities that are also developed by cybercriminals. In general terms, and given the configuration of non-compliance regarding the duty of prevention and security that the banking entity must comply with within the framework of the consumer contract, the punitive damage appears to be entirely appropriate.

Keywords: responsibility – electronic scams – phishing – security and prevention – punitive damage

I. Introito

La temática a comentar nos introduce en el estudio de la responsabilidad bancaria ante la explosión de estafas electrónicas –que, sobre todo, proliferaron durante la pandemia–, cuyas víctimas resultaron ser –en su mayoría– los consumidores de servicios bancarios.

El objetivo de este comentario es centrarnos en los deberes de seguridad y prevención que las entidades tienen frente a sus clientes, obligaciones cuyo cumplimiento, en el marco del contrato de consumo, en muchos casos, no estuvo a la altura de las circunstancias y de la conducta que es esperable por parte de las entidades proveedoras de servicios bancarios; hechos que, en enorme cantidad de casos, originó su inevitable judicialización.

El presente artículo también pretende repensar la aplicación del instituto del daño punitivo al que refiere el art. 52 de la Ley de Defensa del Consumidor en casos en los que la responsabilidad del ente bancario se configura ante estafas electrónicas, su procedencia y cuantía. Finalmente, acercaremos al lector un reciente fallo del Superior Tribunal de Justicia de la Provincia de Jujuy.

II. Responsabilidad de la entidad bancaria ante estafas electrónicas

El interrogante –que es directriz nodal de la temática que exponemos– intenta desentrañar si es posible responsabilizar a las entidades bancarias ante la ocurrencia de estafas electrónicas.

La mayoría de los casos, a partir de los cuales se ha ido sentando jurisprudencia, tiene su origen en estafas sufridas por el consumidor a través de la técnica denominada *phishing* (cosecha y pesca de contraseñas),¹ mediante la cual un ciberdelincuente logra ingresar al *home banking* de aquel, bajo una serie de engaños y manipulaciones, captando fraudulentamente sus datos. De esta forma, una vez en su cuenta, el tercero solicita fraudulentamente un préstamo preaprobado y sustrae o desvía fondos acreditados sin

¹ Cristian Borghello y Marcelo Temperini, “La capacitación ilegítima de datos confidenciales como delito informático en Argentina”, *XLI Jornadas Argentinas de Informática e Investigación Operativa* (agosto de 2012): p. 3. Disponible en: http://sedici.unlp.edu.ar/bitstream/handle/10915/124434/Documento_completo.pdf?sequence=1&isAllowed=y.

consentimiento o autorización del cliente. En ese supuesto, el consumidor se ve expuesto a los correspondientes débitos en su cuenta con motivo de las cuotas que se generan por el préstamo "a un solo click". En otros casos, la estafa también se realiza mediante otras figuras como extracciones o compras virtuales que el ciberdelincuente también tiene a su alcance realizar.

El denominado *phising* es un término relativamente nuevo que forma parte de un fenómeno que parece reinventarse y perfeccionarse constantemente. Con anterioridad a la aparición de la pandemia por Covid-19, los ardides y las maniobras de engaño giraban principalmente sobre la órbita de cajeros automáticos, llamados telefónicos con suplantación de identidad, correos electrónicos falsos o clonación de tarjetas de débito o crédito.

El aislamiento social, preventivo y obligatorio (ASPO), que tuvo lugar durante la pandemia (en algunos momentos con mayor o menor recrudescimiento), provocó un inevitable aumento del uso y acceso a las redes sociales por parte de los usuarios para dar respuesta a sus necesidades.²

El supuesto de hecho del que debemos partir en lo que es materia de análisis radica en sostener que es indiscutible que las operaciones de préstamos y extracciones son realizadas sin participación del consumidor. De manera tal que la completa ausencia de su consentimiento determina que no existió contrato de préstamo o mandato con la entidad bancaria. La falta de voluntaria participación del consumidor en las operaciones lo coloca en una inevitable situación de vulnerabilidad y abuso que la normativa debe tutelar.

El punto basal radica en sostener que es el mismo banco quien ofrece a sus clientes un nuevo modo de relacionarse comercialmente con él, al punto tal de que la mayoría de las gestiones o trámites que el consumidor de este tipo de servicios debe o necesita realizar es impuesta –casi con exclusividad– por canales electrónicos o digitales. De tal modo, surge repotenciada la afirmación de que aquel debe procurar –como mínimo– la misma seguridad que si tal operatoria se realizara personalmente.

² Estos son los datos que informa el Centro Latinoamericano y del Caribe de Información en Ciencias de la Salud (BIREME), según la Organización Panamericana de la Salud. Publicado el 05/05/2020.

Esta seguridad está dada prioritariamente por la confianza que al consumidor le brinda el medio empleado. Confianza que no solo radica en el uso de una clave personal y única, sino también en la esperable inviolabilidad del software utilizado por la entidad.

III. El deber de seguridad y prevención en el marco del contrato de consumo

La obligación de seguridad se desprende directamente del art. 42 de la Constitución Nacional que enumera, entre los derechos básicos de los consumidores, “la protección de su seguridad e intereses económicos”.

Por su parte, el art. 5 de la Ley Nro. 24.240 establece la obligación de seguridad en sentido estricto, el art. 6, el deber de advertencia y el art. 40, la responsabilidad por el riesgo de la cosa.

La era de auge de las nuevas tecnologías y modalidades de contratación electrónicas, digitales e informáticas que transitamos impone a las entidades financieras reforzar la función preventiva que el marco tutelar del consumidor les ha impuesto, tomando concretas y efectivas medidas de seguridad en relación con los servicios digitales que brindan a sus usuarios. En el abanico de servicios que el banco ofrece a sus clientes, tanto para el caso en que fueran llevados a cabo de manera personal o de un modo electrónico, digital o mecánico, existe la intrínseca obligación del proveedor de brindar adecuada tutela al cliente sobre la seguridad de las operaciones, en tanto inciden de manera directa sobre su patrimonio.

No puede la entidad bancaria pretender desentenderse de las consecuencias disvaliosas que acarrea su omisión de contar con adecuadas y sólidas medidas de seguridad en la prestación de servicio de *home banking* que permitan individualizar y garantizar, de manera fidedigna, la identidad del usuario y la confiabilidad de la operatoria que se realiza. Esta tesitura se compadece con la imposición a los bancos de contar con los mecanismos de seguridad informática a los fines de garantizar confiabilidad en operatorias conforme a las Comunicaciones “A” 6878, punto 3.8.5, y “A” 6949 del Banco Central de la República Argentina (BCRA).

Dice Abad que, “a la luz de la normativa consumeril vigente, la responsabilidad del Banco ante las estafas electrónicas bancarias es palpable, atento [la] apariencia de confiabilidad del sistema brindado, en tanto es la propia entidad la que ofrece e impone

el uso de home banking y redes sociales para la comunicación con los consumidores”.³ Así, al momento de elegir la institución bancaria, el usuario deposita la confianza en ella, en el entendimiento de que su dinero se encuentra resguardado y podrá disponer de él cuando quiera.

No nos es ajeno tampoco que el art. 5 de la Ley Nro. 24.240 prevé la denominada garantía de inocuidad por la 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.

Del Texto Ordenado del Banco Central de la República Argentina, en lo que respecta 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" (Requisitos), surge la obligación de la entidad financiera de:

adquirir, desarrollar y/o adecuar los mecanismos implementados para la verificación de la identidad y privilegios de los usuarios internos y externos, estableciendo una estrategia basada en la interoperabilidad del sistema financiero, la reducción de la complejidad de uso y la maximización de la protección del usuario de servicios financieros.⁴

Del mismo modo, los Requisitos obligan a los bancos a implementar “técnicas de detección y prevención de apropiación de datos personales y de las credenciales mediante ataques de tipo 'ingeniería social', 'phishing', 'vishing' y otros de similares características”.⁵

Asimismo, la Comunicación “A” 6878 dispone un punto clave para analizar la responsabilidad de las entidades, para lo que “deberán adoptarse normas y procedimientos internos a efectos de verificar que el movimiento que se registre en las cuentas guarde razonabilidad con las actividades declaradas por los clientes”.

³ “Análisis de la responsabilidad bancaria en casos de estafas electrónicas mediante redes sociales desde la óptica del derecho de consumo”, Gabriela Abad, consultado en abril de 2022. Disponible en: <https://www.abogadovergara.com.ar/2021/05/analisis-de-la-responsabilidad-bancaria.html>.

⁴ “Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras”, Banco Central de la República Argentina”, consultado en abril de 2022. Disponible en: <https://www.bcra.gob.ar/Pdfs/Textord/t-rmsist.pdf>, p. 3.

⁵ “Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras”, p. 15.

Dice Abad que la Comunicación “A” 7319 emitida por el BCRA, que entró en vigencia el 9 de julio de 2021, dispone que:

[p]ara la autorización de un crédito preaprobado la entidad debe verificar fehacientemente la identidad de la persona usuaria de servicios financieros involucrada. Esta verificación debe hacerse mediante técnicas de identificación positiva, de acuerdo con la definición prevista en el glosario y en el requisito técnico operativo específico (RCA040) de estas normas. Asimismo, se deberá constatar previamente a través del resultado del proceso de monitoreo y control, como mínimo, que los puntos de contacto indicados por el usuario de servicios financieros no hayan sido modificados recientemente. Una vez verificada la identidad de la persona usuaria, la entidad deberá comunicarle -a través de todos los puntos de contacto disponibles- que el crédito se encuentra aprobado y que, de no mediar objeciones, el monto será acreditado en su cuenta a partir de las 48 horas hábiles siguientes. El citado plazo de acreditación podrá ser reducido en el caso de recibirse la conformidad del usuario de servicios financieros de manera fehaciente.⁶

La citada autora aporta que, más allá de las consideraciones que se pueden realizar sobre esa disposición, resulta novedosa la reflexión judicial sentada por la Oficina de Gestión Judicial en las Relaciones de Consumo del juzgado Nro. 22 de la Ciudad de Buenos Aires en autos "C., R. L. c/ Banco Macro Sociedad Anónima s/ relación de consumo", del 12 de julio de 2021, en cuanto dispone que:

[e]n nada modifica lo expuesto el hecho de que la Comunicación "A" 7319 tenga como fecha de entrada en vigencia el 9 de julio de 2021, ya que la misma pone en evidencia y viene a reconocer las problemáticas referidas a la gestión informática y de seguridad relacionados con el sistema de créditos preaprobados (*sic*).

De esa manera, sienta una importante postura en cuanto a la relevancia de esa reciente medida, que deviene como resultado de una ola de estafas virtuales y la necesidad de ajustar las medidas de seguridad de los bancos que, hasta la fecha, no habían implementado cambios de este estilo para frenar los delitos, por lo que fue necesario el dictado de una normativa de la Autoridad de Contralor a tales fines.

El BCRA, en su página web, publicó un artículo titulado “Lineamientos sobre ciberseguridad” instando a las entidades financieras, los terceros y todo el sector financiero a “establecer estrategias y adoptar un marco de ciberseguridad acorde a su tamaño, complejidad, perfil de riesgo y cultura, teniendo en cuenta las amenazas y

⁶ “Responsabilidad bancaria ante estafa electrónica. Medida cautelar a favor del consumidor”, Gabriela Abad, consultado en abril de 2022. Disponible en: <https://cutt.ly/6J4Oqwx>.

vulnerabilidades actuales”.⁷ En él, hizo hincapié, por un lado, en el análisis del riesgo presentado por las personas, procesos, tecnologías y datos subyacentes con relación a la propia entidad y, por el otro, en la evaluación de los riesgos propios de una entidad a partir de sus funciones, actividades, canales, productos y servicios. También enfatizó en el proceso de monitoreo, el cual “debería dar soporte para mantener los niveles de riesgo definidos como aceptables por la dirección de la organización y permitir mejorar o remediar las debilidades que corresponda”.⁸ A mayor abundamiento, peticona que las entidades implementen “procesos de respuesta a incidentes y otros controles para facilitar una respuesta oportuna y adecuada”.⁹

En relación con la Comunicación “A” 7319 antes mencionada, ha sostenido recientemente la jurisprudencia que no “incide la eventual negligencia o inexperiencia de la actora frente al suministro voluntario de datos, ya que la concurrencia eventual de responsabilidades no puede liberar al banco de los deberes generales de seguridad por él debidos”.¹⁰

En ese sentido también se dijo que:

la prevención en el derecho del consumidor encuentra sustento directo en lo dispuesto en el artículo 42 de la Constitución Nacional [...] en el primer párrafo del mentado artículo se hace referencia a la protección de la seguridad del consumidor. Al respecto, la misma Corte Suprema de Justicia de la Nación sostuvo en el caso «Ledesma» (arg. fallo 331:819) que la seguridad era un valor que debía guiar la conducta de los proveedores de aquellas actividades que se vinculen con la vida o la salud de las personas. En igual sentido, ampliando el alcance dado, en el otro fallo «Uriarte» (333:203), donde la Corte Suprema desarrolló aun más el deber de seguridad. En este sentido, el Alto Tribunal sostuvo que las empresas tienen el deber de extremar las previsiones para el estricto cumplimiento de las leyes y reglamentos dictados en amparo de las posibles víctimas para quienes, de lo contrario, el resarcimiento resultaría ilusorio en la mayoría de los casos. Por consiguiente, la interpretación que hizo el Alto Tribunal sobre el deber de seguridad que se halla incorporado en el artículo 42 de la Carta Magna conlleva la obligación del proveedor de la adopción de las medidas razonables de prevención a los fines de evitar el daño del consumidor. Así, cobra especial relevancia lo establecido en el artículo 1710, incisos b) y c) del CCC en lo que respecta la protección de los derechos de los

⁷ “Lineamientos sobre ciberseguridad”, Banco Central de la República Argentina, consultado en abril de 2022. Disponible en: <http://www.bcra.gov.ar/SistemasFinancierosYdePagos/Ciberseguridad.asp>.

⁸ “Lineamientos sobre ciberseguridad”.

⁹ “Lineamientos sobre ciberseguridad”.

¹⁰ Es la línea argumental que se ha sostenido por la Secretaría Nro. 2 de la Oficina de Gestión Judicial en las Relaciones de Consumo del Juzgado Nro. 22 del Poder Judicial de la Ciudad de Buenos Aires, en autos “C. R. L. c/ Banco Macro Sociedad Anónima s/ relación de consumo” (12/07/2021).

consumidores. En este sentido, resulta aplicable al proveedor la obligación específica de adoptar medidas de seguridad a los fines de evitar la producción del daño, es decir, se encuentra obligado a invertir en aquellas medidas de seguridad para prevenir el daño en los consumidores o, en el caso en que detecte productos defectuosos en el mercado, adopte las medidas necesarias para cesar o disminuir los eventuales daños.¹¹

La Sala B de la Cámara de Apelaciones de Trelew se ha expedido en este sentido

[e]n los últimos tiempos, debido a la alta concentración e intensa concurrencia en la actividad bancaria, a lo que se suma el desarrollo de la nueva tecnología, se ha configurado un mercado bancario novedoso y dinámico, con productos que se podrían llamar no tradicionales como las tarjetas de débito, el dinero digital, el e-banking, los sistemas de atención telefónica, etc. Estos productos o servicios bancarios que dan contenido a las denominadas operaciones neutras lejos de no producir beneficios económicos a los bancos son muchas veces de las más importantes fuentes de ingresos, sino las más importantes... En la actualidad, los servicios bancarios son más que un elemento instrumental, ya que se han convertido en una finalidad de la comercialización bancaria que responde a los nuevos hábitos de los partícipes del sistema bancario en general [...] La perspectiva del riesgo empresario desde la óptica jurídica implica su traducción en el deber de seguridad que corresponde asignar sin dudar que pesa sobre las entidades bancarias intermediadoras en el mercado del dinero. Es que no puede quedar de lado en tal hermenéutica que para la viabilidad de dicha intermediación debe ponderarse que concurre una obligación tácita de seguridad, que confluye con la confianza como valor intrínseco que como pilar básico de todo mercado, es connatural a la actividad bancaria.

La Sala D de dicho Tribunal se pronunció también:

no es posible superar la responsabilidad del Banco demandado con la sola invocación de haber sido víctima de la actuación de un tercero por el cual no tiene que responder ya que su inexcusable omisión es razón suficiente para responsabilizarlo... La mera invocación del hecho de un tercero resulta ineficaz para lograr la exención de responsabilidad, si no se configuran los extremos propios del caso fortuito que atañen a la imprevisibilidad e inevitabilidad del hecho, siendo claro, en tal sentido, que el ilícito derivado de la sustitución de persona de que se trata no sólo no puede calificarse de imprevisible, sino que especialmente no puede catalogarse como inevitable en la medida que, ciertamente, se cumplan con los recaudos exigidos reglamentariamente para constatar adecuadamente la identidad de quien, como en el caso de autos, se presenta a solicitar un préstamo.

¹¹ Es la tesis expuesta por el Juzgado Civil y Comercial de La Plata, Sala/Juzgado: XVIII, en Expte. “Suárez González María Piedad c/ Banco de la Provincia de Buenos Aires s/ nulidad de contrato”, 24/09/2020.

El Superior Tribunal de Justicia de la Provincia de Jujuy en sentencia registrada en Libro de acuerdos Nro. 2, Nro. de Registro Nro. 102 dijo:

[e]s que, la regulación de la actividad financiera requiere conjugar las exigencias de alta profesionalidad y de la plena satisfacción de la confianza de los clientes bancarios, quienes constituyen la parte débil en la relación contractual y la depositan en las entidades, en función del alto grado de especialización que tienen en la prestación del servicio; deben actuar regidas por el estándar ético del buen profesional, dado que son, asimismo, colectoras de fondos públicos, y el interés general exige que actúen con responsabilidad, debiendo considerarse que el principio de confianza, aunque no textualizado, es de orden público y se vincula con la protección del cliente para el mantenimiento de la transparencia y credibilidad entre la oferta y la contratación financiera.

IV. Daños punitivos: procedencia y cuantía del *casus* concreto

Como es sabido, cada caso particular amerita una ponderación específica en la que – conjugadas las circunstancias fácticas con el derecho aplicable en el marco de la sana crítica racional– el operador jurídico pueda determinar la procedencia o no del instituto del daño punitivo y, en su caso, su cuantía.

En líneas generales, y ante la configuración del incumplimiento en lo que es materia propia del deber de prevención y seguridad que el ente bancario debe cumplir en el marco del contrato de consumo, el daño punitivo resulta enteramente procedente. Esto es así ya que la sanción punitiva en el derecho del consumidor se explica por la función de tutela que la Ley Nro. 24.240 atribuye al Estado a los efectos de disuadir a las empresas proveedoras de incurrir en conductas reiteradas que lesionen los bienes jurídicos protegidos por dicha normativa.

El juez, en su tarea hermenéutica, deberá sopesar los elementos propios que enmarcan cada caso particular y que conforman la plataforma fáctica o sustrato empírico sobre el que debe decidir. Resultan imaginables un sinnúmero de situaciones particulares que podrán presentarse en los estrados judiciales (muchas de ellas, verdaderamente, ya han sido materia de debate y decisión).

La procedencia o el rechazo del daño punitivo podrá variar según que la entidad bancaria haya o no incurrido en un incumplimiento grave que refleje la falta de trato digno hacia el consumidor, o haya faltado a la buena fe y al deber de información veraz que también debe cumplir.

El incumplimiento puede presentar muchísimos matices. En algunos supuestos, la jurisprudencia ha decidido sobre diversas cuestiones en las que la entidad bancaria se negó a restituir al cliente las sumas de dinero por las que fue estafado. En otros, se produjo el reintegro del dinero, pero con una dilación tal que igualmente afectó los derechos del consumidor pues habiéndose producido el reintegro de las sumas, la entidad bancaria sostenía que ningún interés le debía al consumidor. En ciertos casos –por no decir en todos– el peregrinar del usuario de servicios bancarios se vio potenciado por la circunstancia de que la atención personalizada era inexistente en tiempos de pandemia o, al menos, se encontraba restringida. De todos modos, el consumidor debía solicitar turno para recibir una atención personalizada, turno que difícilmente se otorgaba con la premura que la cuestión ameritaba.

Algunas otras explicaciones brindadas, que dilataron la respuesta de la entidad bancaria ante los reclamos de los consumidores, fueron las que se ensayaron en torno a la disponibilidad de la vía *online* para reclamos y vías telefónicas.

Lo cierto es que los incumplimientos de las entidades bancarias en su obligación de prevención y seguridad pueden hacer menester la imposición de la multa civil para disuadir futuras inconductas que consagren un claro menosprecio hacia el sujeto débil de la relación consumeril que la norma ha querido tutelar.

El consumidor tiene el derecho a ser tratado con cortesía, corrección y diligencia, y a obtener una respuesta adecuada y oportuna a su requerimiento. Todas estas son notas típicas de la relación de consumo que, si se evidencian ausentes en el caso concreto, tornan plenamente procedente la aplicación del instituto contenido en el art. 52 bis de la Ley de Defensa del Consumidor, máxime cuando –como en muchos casos– se acompaña del silencio y la falta de solución pronta a los innumerables reclamos cursados del consumidor, y lo obliga a iniciar acciones en la instancia judicial para articular la pretensión resarcitoria con el fin de obtener la reparación de los daños efectivamente sufridos como consecuencia del incumplimiento.

Debe tenerse presente, al momento de cuantificar el daño punitivo, que la sanción debe ser particularmente ejemplificadora para que se cumpla la función punitiva, preventiva y disuasiva que el legislador ha querido imprimirle al instituto. La multa debe guardar condigna sanción, lo que implica que esta debe resultar adecuadamente proporcional, de manera tal que la aplicación del instituto resulte racional y prudente;

teniendo presente que una interpretación razonable de la norma exige su adecuación a los principios informadores del derecho privado y el resguardo de derechos constitucionales.

Los daños punitivos, en realidad [...] son de naturaleza pecuniaria disuasiva/punitiva, en tanto se transforma en un elemento adicional a la hora de sancionar al victimario y evitar futuras conductas dañosas [...] Se puede distinguir en el daño punitivo una función principal y otra accesoria. La principal es la disuasión y la causación de daños conforme con los niveles de precaución deseables socialmente. La función accesoria es la sanción al dañador, ya que toda multa civil, por definición tiene una función sancionatoria en oposición a la indemnización por daños y perjuicios que es compensatoria.

V. Un reciente antecedente del Superior Tribunal de Justicia de Jujuy

Recientemente, el Superior Tribunal de Justicia de Jujuy se pronunció sobre un recurso de inconstitucionalidad interpuesto contra la sentencia "Acción Emergente de la Ley del Consumidor: C.A.M. c/ Banco Macro S.A." de la Sala II de la Cámara en lo Civil y Comercial jujeña. Allí se dijo que:

[a] partir de esta relación de consumo puede ponderarse -prima facie- una evidente asimetría entre las posibilidades del cliente consumidor y las de la entidad bancaria prestadora del servicio en punto a la conducta que es dable esperar de cada uno de ellos en el desarrollo del vínculo contractual. Por ello es que a los contratos bancarios celebrados con consumidores y usuarios les son aplicables las disposiciones relativas a los contratos de consumo (art. 1384 del C.C.C.N.) [...] considero que la entidad bancaria no puede pretender desentenderse de la situación con solo alegar que el actor/consumidor reconoció haber sido víctima de phishing y que ello ocurrió por su exclusiva culpa. Es que, bajo la tutela judicial efectiva que ampara al consumidor (arts. 42/43 de la C.N. y 73 de la C.P.) no puede permitirse que con tanta liviandad el proveedor sortee la responsabilidad que pueda corresponderle en la ocasión [...] aún cuando fuere verdad que el accionante fue negligente y comprometió de algún modo información personal, lo innegable es que falló el sistema de seguridad del Banco al permitirle a un tercero suscribir una contratación en su nombre.

Fue terminante el Alto Tribunal cuando expresó que:

[n]o debe pasar inadvertido que el Banco, en tanto proveedor del servicio, debió en todo momento brindar a su cliente información cierta, clara y detallada, acerca de los peligros a los que se sometía al utilizar su cuenta en el home banking (cfr. arts. 4° de la L.D.C. y 1100, 1106 y 1107 del C.C.C.N.) [...] Es que, esta información no solo debe ser adecuada y veraz sino también 'oportuna'; esto es, que sea brindada constantemente mientras dure el contrato bancario que vincula a las partes, de modo que el consumidor cuente con la información útil y necesaria para ejecutar las operaciones que desee a través del home banking sin ser luego víctima de estafas, fraudes, etc.

Resultan interesantes los términos del dictamen del Ministerio Público que en la sentencia se tienen por reproducidos como parte integrante de esta. Respecto a los incumplimientos en los que incurre la entidad bancaria y que fundan la procedencia del daño punitivo, sostuvo que:

[s]obre la particular apreciación de la entidad accionada de que la vía telefónica estuvo siempre a disposición del actor, cabe precisar que no ha desvirtuado ni negado las aserciones del mismo, en tanto éste alegó haber intentado en numerosas oportunidades establecer el contacto telefónico con el centro de atención al cliente y haber concurrido personalmente al Banco en busca de una solución al problema. Todos ellos, intentos infructuosos de los que la demandada no se hace cargo y que -per se- traducen un claro detrato hacia el consumidor que patentiza una conducta alejada de los parámetros que la exigencia de la norma respecto al trato digno al consumidor y buena fe ha querido reflejar en el marco tuitivo que nos convoca. Caben idénticas apreciaciones sobre el silencio que el Banco mantuvo ante la intimación fehaciente que cursó el actor.

VI. Corolario

Resulta valioso desde el plano axiológico apreciar que existe una marcada tendencia en la jurisprudencia –a lo largo de todo el país– de resaltar y poner en valor el deber de seguridad y prevención que pesa sobre las entidades bancarias respecto de los usuarios y consumidores.

La responsabilidad civil de los bancos se pone en relieve toda vez que, frente al acaecimiento de cada estafa electrónica, los consumidores encuentran vulnerados sus derechos a la seguridad, información y protección de los intereses económicos, consagrados tanto en la Constitución Nacional como en la Ley Nro. 24.240 y en el Código Civil y Comercial de la Nación, que, a su vez, son deberes propios de las entidades bancarias.

Conforme a los fines de la normativa del BCRA de prevenir y detectar tempranamente la apropiación ilegítima de datos personales de los usuarios bancarios, resulta ineludible para las entidades bancarias dar acabado cumplimiento al deber de concientización y capacitación de seguridad informática.

En líneas generales, y ante la configuración del incumplimiento del deber de prevención y seguridad que tiene el ente bancario en el marco del contrato de consumo, el daño punitivo resulta enteramente procedente, más allá de las particularidades y

matices que cada caso pueda presentar en lo que respecta a la procedencia *strictu sensu* o a la determinación de su cuantía.

En los tiempos de auge de nuevas y modernas tecnologías, resulta imperioso que los bancos intensifiquen los recaudos para una efectiva prevención y concientización ante ataques de ciberdelincuentes que, constantemente, modernizan los mecanismos de búsqueda y captación de datos, claves personales y contraseñas de sus clientes.

Bibliografía

- Abad, Gabriela A. “Análisis de la responsabilidad bancaria en casos de estafas electrónicas mediante redes sociales desde la óptica del derecho de consumo”. Disponible en: <https://www.abogadovergara.com.ar/2021/05/analisis-de-la-responsabilidad-bancaria.html>.
- Abad, Gabriela A. “Responsabilidad bancaria ante estafa electrónica. Medida cautelar a favor del consumidor”. Disponible en: <https://cutt.ly/6J4Oqwx>.
- Banco Central de la República Argentina. “Lineamientos sobre ciberseguridad”. Disponible en: <http://www.bcra.gov.ar/SistemasFinancierosYdePagos/lineamientos-de-ciberseguridad.asp>.
- Banco Central de la República Argentina. “Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras”. Disponible en: <https://www.bcra.gov.ar/Pdfs/Textord/t-rmsist.pdf>.
- Borghello, Cristian y Temperini, Marcelo. “La capacitación ilegítima de datos confidenciales como delito informático en Argentina”. XLI Jornadas Argentinas de Informática e Investigación Operativa (agosto de 2012): pp. 94-108. Disponible en: http://sedici.unlp.edu.ar/bitstream/handle/10915/124434/Documento_completo.pdf?sequence=1&isAllowed=y.
- Cámara de Apelaciones de Trelew, Sala B, “Dirección General de Defensa del Consumidor y Protección de Derechos c/ Banco de Galicia y Buenos Aires S.A. s/ contencioso administrativo – presunta infracción Ley 24.240”, Expte. Nro. 590, 11/02/2010.

Cámara de Apelaciones de Trelew, Sala D, “García Rita Cynthia Noemí c/ Banco Columbia S.A. s/ ordinario”, 20/10/20.

Gozaíni, Osvaldo Alfredo. *Debido proceso*. Buenos Aires: Ed. Rubinzal Culzoni, 2004.

Juzgado Civil y Comercial de La Plata, Sala XVIII, “Suárez González Maria Piedad c/ Banco de la Provincia de Buenos Aires s/ nulidad de contrato”, 24/09/2020.

Organización Panamericana de la Salud. “Las redes sociales y COVID-19: la contribución de BIREME”. Disponible en: https://www.paho.org/bireme/index.php?option=com_content&view=article&id=479:redes-sociais-e-covid-19-a-contribuicao-da-bireme&Itemid=183&lang=es.

Secretaría Nro. 2 de la Oficina de Gestión Judicial en las Relaciones de Consumo del Poder Judicial de la Ciudad de Buenos Aires, Juzgado Nro. 22, “C. R. L. c/ Banco Macro Sociedad Anónima s/ relación de consumo”.

Superior Tribunal de Jujuy, L.A. 2, Nro. 102, Expte. CF-12.591/16, “Recurso de Inconstitucionalidad interpuesto en B-264.458/11 (Cámara en lo Civil y Comercial -Sala II- Vocalía 5) Ordinario por daños y perjuicios: Salum, Andrés Alejandro c/ Banco Santander Río S.A.”.

Superior Tribunal de Jujuy, L.A. 6, Nro. 401, Expte. CF-17.647/21, “Recurso de inconstitucionalidad interpuesto en el Expte. Nro. C- 170.561/2020 (Cámara en lo Civil y Comercial- Sala II- Vocalía 5), caratulado: “Acción Emergente de la Ley del Consumidor: C.A.M. c/ Banco Macro S.A.”.