UNIVERSIDAD NACIONAL DEL NORDESTE

FACULTAD DE DERECHO Y CIENCIAS SOCIALES Y POLÍTICAS
UNIVERSIDAD NACIONAL DEL NORDESTE

MAESTRÍA DE DERECHO EMPRESARIO

Responsabilidad Civil Bancaria Frente a Clientes Víctimas de Ilícitos Informáticos Cometidos por Terceros

Alumno: Raúl Manuel de Jesús Narváez

Director: Dr. Edgardo Darío López Villagra

Corrientes, agosto de 2023

Dedicatoria

A mis padres que un día partieron de esta vida y me dejaron la fortaleza, de continuar siempre adelante, sin importar los riesgos, son mis paradigmas de vida, honestidad, trabajo, dignidad y amor. Ellos fueron mi fuente y razón de vida.

A mi familia esposa e hijos: Gladys, Yahíra y Alejandro, por darme el apoyo, la fueza y aguante en todo este tiempo. Los amos.

A todos mis hermanos por los consejos, tolerancia y apoyo incondicional. en especial a mi hermano Beto que fue mi compañero y amigo que ya no está y lo extraño mucho. Los quiero a lo que están y aquel en cualquier lugar que esté.

A mis compañeros, amigos, que dieron su granito de arena, para que yo esté en esta etapa tan ansiada. Gracias.

Agradecimientos

A dios que es la fuente de razón y existencia, que toda persona encuentra la fortaleza en su apoyo su resguardo amor, guiado por esa fe infinita.

A mis profesores de la Universidad que abrieron la puerta de tanto conocimiento, a mi tutor de tesis Rubén Darío López Villagra y su señora Adriana, por la orientación y amabilidad que siempre y todo momento que tuvieron.

A mis cuñados Norma y Marcelo Olivera; al amigo Daniel, que me apoyaron, ayudaron y guiaron durante la realización del trabajo final, sin sus apoyos no hubiera sido posible terminarlo.

A la Dra. Manferrer y su secretaria Agustina, por su disponibilidad, amabilidad, en todas las consultas, también por su aliento en todo momento, en la realización del presente trabajo.

A todos de alguna u otra manera que pusieron su granito de arena para que esto se haga realidad. Gracias.

Índice

Abreviaturas Empleadas

AFIP: Administración Federal de Ingresos Públicos

art./arts.: artículo/artículos

BID: Banco Interamericano de Desarrollo

BCBS: Basel Committee on Banking Supervision

BCRA: Banco Central de la República Argentina

BCU: Clave Bancaria Uniforme

CABA: Ciudad Autónoma de Buenos Aires

CBP: Clave Bancaria Previsional

CC: Código Civil

CNCiv: Cámara Nacional Civil

CNV: Comisión Nacional de Valores

CP: Código Penal

CPCC: Código Procesal Civil y Comercial

CSJN: Corte Suprema de Justicia de la Nación

DEBIN: Medio de pago Débito Inmediato

DNI: Documento Nacional de Identidad

EEUU: Estados Unidos

FINTECH: Financial Technology

IA: Inteligencia Artificial

ICBC: Industrial And Commercial Bank of China

inc.: inciso

IoT: Internet Of Things

IP: Internet Protocol

LDC: Ley de Defensa del Consumidor

LEF: Ley de Entidades Financieras

LL: Colección La Ley

N°/Nro.: Número

NBU: Normas Bancarias Uniformes

O.D.I.A.: Observatorio de Derecho Informático Argentino

PEN: Poder Ejecutivo Nacional

PPM: Plataforma de Pagos Móviles

SEFC: Superintendencia de Entidades Financieras y. Cambiarias

SEFyC: Superintendencia de Entidades Financieras y Cambiarias

SMS: Short Message System

STJ: Tribunal Superior de Justicia

T-CY: Comité del Convenio sobre la Ciberdelincuencia

TICs: Tecnologías de la Información y de la Comunicación

UE: Unión Europea

Introducción

Vivimos en una etapa histórica de vertiginosa evolución tecnológica en la cual la innovación avanza a un ritmo cada vez mayor y repercute en todos los ámbitos de la actividad humana. No resulta sorprendente que en esta nueva era de digitalización, inteligencia artificial y automatización, las personas y las organizaciones se vean obligadas a actualizar sus prácticas y operaciones para asimilar esos cambios de contexto.

Frente a la omnipresencia de las nuevas Tecnologías de la Información y la Comunicación (TIC) que han impregnado todas las esferas de la sociedad, el ámbito jurídico no ha sido una excepción. La relación entre tecnología y derecho se ha hecho cada vez más estrecha, y plantea oportunidades y desafíos diversos. Parece indudable que el avance tecnológico acelerado provoca la necesidad de revisar la conceptualización jurídica clásica y sugiere adoptar una perspectiva comprensiva e integral del fenómeno.

El empleo de las TIC y los riesgos que entraña son motivo de preocupación para algunos sectores de la sociedad, sobre todo en lo referido a la seguridad patrimonial de los usuarios de los modernos sistemas de comunicación. La posibilidad de manejar información sensible de sujetos y organizaciones usando tecnologías capaces de adquirir, procesar y transmitir datos, que unas décadas atrás sólo podía concebirse como producto de la imaginación de los autores de novelas distópicas ─*1984* (George Orwell, 1948)─ o de ciencia ficción ─*Mundo Anillo* (Larry Niven, 1970)─[1]. actualmente forma parte de la realidad cotidiana, y expone a todas las personas a situaciones de riesgo.

En relación con el uso de la tecnología para captar información, se recuerda que, a principios de la década de 1980 ocurrieron en EEUU casos de alteración de archivos de bases de datos y balances de empresas y entidades bancarias, buscando manipular recibos

[1] V. Caramuto Martins, G. (2013). *Influencia de la Ciencia Ficción en las TIC y las Telecomunicaciones*. Trabajo Fin de Carrera/Grado. E.U.I.T. Telecomunicación (UPM) [antigua denominación], Madrid, https://oa.upm.es/20938/

salariales. El modus operandi consistía en la instalación de dispositivos lectores en la entrada de cajeros automáticos, colocando teclados falsos adentro de ellos para copiar los datos de las tarjetas de débito. Esto condujo a las empresas emisoras a instalar chips en los plásticos como medida de seguridad (Saín, 2018). Como expresa Saín (2015, citado en Saín, 2018, p. 8):

> Fue justamente durante esta época donde comienza la protección normativa de los países europeos a los bienes inmateriales como el dinero electrónico, […]. La cobertura legal de las bases de datos de las instituciones bancarias y empresas resultaba indispensable para la realización de negocios, fundamentalmente contra el robo de información comercial.

Con la apertura de internet a mediados de la década de 1990 en EEUU y su posterior expansión global, las conductas delictivas comenzaron a adquirir una nueva dimensión, sobre todo a partir de la masificación de dispositivos informáticos ─teléfonos móviles, computadoras, tabletas y consolas de juegos, entre otros─ que permiten enviar, recibir y transmitir información mediante el uso de un protocolo común de comunicaciones (Saín, 2018).

Estas características impulsaron la expansión de las TIC, y especialmente de Internet, que actualmente ha llegado a ser el medio cibernético más utilizado para la comunicación de millones de personas y empresas alrededor del planeta. Los bancos comenzaron a diseñar estrategias para usar esta red en sus operaciones, animados por las indudables ventajas que ofrece para la actividad financiera.

El acceso masivo a este universo en constante crecimiento trajo consigo un nuevo paradigma disruptivo, ya que las entidades bancarias ─al igual que otras instituciones de la sociedad─ también optaron por implementar reformas tendientes a usar nuevos servicios electrónicos para llevar a cabo diferentes operaciones. Las empresas del sector fueron

transformando sus operatorias y se modificó de manera sustancial la forma de ofrecer ─y por ende, de consumir─ los servicios y productos financieros

La interacción entre los bancos y sus clientes fue evolucionando significativamente con la adopción de plataformas digitales y servicios en línea. Estas y otras innovaciones tecnológicas han generado una mayor comodidad y accesibilidad para los usuarios, permitiéndoles realizar diversas transacciones financieras mediante dispositivos móviles y otras herramientas digitales, sin tener que concurrir al establecimiento.

No resulta exagerado afirmar, en ese orden de ideas, que la naturaleza multifacética de la tecnología ha rediseñado la arquitectura misma del sistema bancario. La rápida transición desde las transacciones tradicionales hacia las realizadas en medios electrónicos ha revolucionado la dinámica interna de los bancos, y la interacción entre éstas y sus clientes

Los distintos medios electrónicos empleados en la actividad bancaria abarcan un amplio catálogo, desde la banca por internet hasta la banca móvil y el uso de cajeros automáticos. Esta metamorfosis tecnológica impulsa la eficiencia operativa y facilita la accesibilidad a los servicios, pero también conlleva el surgimiento de un cúmulo de desafíos legales, sociales, económicos y culturales. La responsabilidad en caso de fallos tecnológicos, la posible vulnerabilidad de sistemas y usuarios frente a los ataques cibernéticos y la necesidad de protección de estos, asoman como cuestiones cardinales de indudable interés y actualidad.

En tal sentido, la simbiosis entre la civilización humana y el rápido avance de la tecnología ─respecto de la que tanto individuos como organizaciones demuestran una creciente dependencia─ ha determinado como mayor desafío la expansión de la ciberdelincuencia, que abarca cualquier actividad ilegal que se lleva a cabo a través de medios electrónicos como la computadora, el teléfono o Internet.

Una amplia gama de individuos y grupos ─desde delincuentes individuales hasta organizaciones criminales internacionales─ buscan aprovechar la situación de manera fraudulenta para obtener réditos económicos. El cibercrimen se ha convertido en un problema de escala mundial, y la necesidad de abordarlo para prevenir su aparición y afrontar sus consecuencias se hace cada vez más urgente. La ciberdelincuencia afecta directamente a los usuarios y consumidores y plantea serios desafíos al sistema financiero y también a la sociedad en general. Se apunta al respecto, que los gastos generados por los ciberdelitos representan cifras cuantiosas para todas las naciones del planeta, generando una preocupación creciente que ha llevado a diseñar estrategias y emprender acciones para afrontar la problemática (BID y OEA, 2020).

La banca electrónica ofrece la ventaja de eliminar las restricciones temporales y geográficas tradicionalmente asociadas a la operatoria de los bancos. Sin embargo, la exposición a fraudes, el acceso no autorizado a cuentas y la posible interrupción del servicio que ocurre cada vez con más frecuencia, plantean diversos interrogantes. La banca es muchas veces un coto de caza favorable para la comisión de actividades fraudulentas, aprovechado por sujetos que explotan las vulnerabilidades de sistemas y personas.

Lo expuesto conduce a pensar que la mayor facilidad en la transmisión de datos y la ejecución sencilla de operaciones financieras mediante plataformas electrónicas requiere de un entorno seguro para evitar situaciones que perturben al sistema y afecten los negocios y, sobre todo, los derechos de las partes involucradas, por lo que se deben implementar medidas preventivas eficaces.

El ámbito de las instituciones bancarias es un terreno especialmente fértil para la propagación de la ciberdelincuencia. En tal sentido, el informe "Fraude digital en la banca 2021" (BTR, 2022) ─que analizó casos reales de estafas bancarias, definiendo sus características fundamentales y las modalidades más ejecutadas durante 2020-2021─ advierte

que "más del 50% de los bancos de todo el mundo experimentaron aumentos en el número y la cuantía de los fraudes de ejecución externa". El informe destaca, además, que durante 2020 se identificaron 130 estratagemas de fraude distintas y, en el primer trimestre de 2021, se descubrieron otras 90 nuevas formas de estafas on-line que afectan a las entidades financieras y sus clientes, entre las que se mencionan el robo de identidad, la toma de control de cuenta y las estafas de pagos automáticos. (BTR, 2022).

Basta mencionar algunos datos referidos en particular a nuestro país para completar ese cuadro: según el CEDIP (2022), el 91.2% de la población argentina cuenta con acceso a internet y la Argentina ─que adhirió al Convenio de Budapest Sobre Ciberdelito del Consejo de Europa (15 de diciembre de 2017) el 5 de junio de 2018─.se ubica en la posición 91 del Índice Global de Ciberseguridad 2020 de la UIT, (Ley 27.411, BO, 2018).

En tanto, durante la pandemia de COVID-19 en 2020, las estafas electrónicas se incrementaron, aprovechando las restricciones de atención presencial en entidades financieras. Por otra parte, la Asociación Argentina de Lucha contra el Cibercrimen reportó un aumento del 65% en los ciberdelitos, incluyendo estafas bancarias que representaron alrededor del 40% de ellos. Con respecto a lo ocurrido en el sector bancario, las estafas se acentuaron debido a la situación creada a partir de los préstamos precalificados ofrecidos a través de homebanking por los bancos, que carecen de medidas de seguridad efectivas. Esto evidenció la fragilidad de la participación de los hogares en el sistema financiero, a menudo carente de información y asesoramiento, lo que los hace vulnerables a diversas actividades delictivas (Luzzi, 2022, pp. 23-24).

El Centro Nacional de Respuesta a Incidentes Informáticos de la Argentina (CERT.ar) registró un total de 591 ataques durante 2021, cifra 261% mayor a la del 2020, siendo relevante mencionar el hecho de que el 55% de los incidentes reportados correspondieron a *phishing*, que es la modalidad más utilizada y será explicada en el capítulo II. Los

ciberataques más dañinos que se registraron fueron por *ransomware* (*software* malicioso), los cuales afectaron principalmente a organizaciones privadas y públicas, y dentro de estas últimas, a las del sector financiero en especial (DNC, 2022).

Teniendo en cuenta lo expuesto, las instituciones públicas han llevado a cabo campañas para educar a la ciudadanía en temas de ciberseguridad. Por ejemplo, *Internet Sano* del Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC), a cargo de la Jefatura de Ministros, se centra en mejorar las prácticas para un uso seguro de internet, y *Con Vos en la Web*, conducido por el Ministerio de Justicia y Derechos Humanos, se ha buscado desarrollar competencias para una adecuada ciudadanía digital a través de recomendaciones y tutoriales sobre el uso seguro de internet y las redes sociales (CEDIP, 2022).

Sin embargo, no puede escapar al análisis que, a medida que la tecnología evoluciona se descubren nuevas formas de explotarla para obtener beneficios ilícitos. Las distintas variantes de criminalidad digital son cada vez más sofisticadas, complejas y difíciles de prevenir, sobre todo por los consumidores de servicios financieros sin experiencia en la operatoria en línea, como sucede con personas de edad avanzada, a las que el ordenamiento protectorio de los consumidores considera hipervulnerables.

En vista de lo expuesto, se advierte que esta problemática involucra no sólo al derecho penal, al derecho civil y al derecho de los consumidores, sino al sistema jurídico en conjunto. Respecto al derecho de daños en particular, se han desarrollado una serie de controversias en torno a la responsabilidad imputable a las entidades bancarias por los perjuicios sufridos por sus clientes como consecuencia de los fraudes cibernéticos cometidos por ciberdelincuentes que aprovechan situaciones de vulnerabilidad para obtener réditos ilícitos.

Las maniobras fraudulentas en el ámbito bancario tienen como víctimas a clientes de las entidades financieras que son engañadas y brindan los datos de sus cuentas bancarias a ciberdelincuentes que extraen de ellas los fondos depositados. En ocasiones, incluso, los autores de los ciberdelitos consiguen que los bancos otorguen préstamos a nombre de los clientes reales, y retiran inmediatamente las sumas de dinero (Saires y María, 2022).

Por lo general, cuando las víctimas reclaman a los bancos, estos niegan su responsabilidad y argumentan que han cumplido con sus obligaciones. Explican que no intervienen en las operaciones que se llevan a cabo en las plataformas electrónicas que ofrecen, siendo sólo intermediarios, porque los clientes pueden operar en ellas con sus cuentas. Además, sostienen que es responsabilidad de los usuarios no brindar sus datos a terceros, asegurando que las medidas de seguridad que adoptan son suficientes y brindan información adecuada al respecto (Saires y María, 2022). Estos desacuerdos terminan llegando a los tribunales, donde los perjudicados accionan en contra de las entidades bancarias.

En este contexto, la delimitación precisa de las obligaciones y responsabilidades de la parte demandada en estos casos ─los bancos comerciales y otras entidades que operan en el sector financiero─ reviste gran relevancia. El análisis de los alcances y límites de la responsabilidad bancaria y el encuadre pretoriano realizado sobre la cuestión resulta ineludible, ya que no existe un sistema regulatorio uniforme al respecto, sino un amplio abanico normativo aplicable, lo que exige determinar un criterio adecuado general para resolver.

Así, en el siempre cambiante escenario en el que las reglas y principios jurídicos se entrelazan con la complejidad y diversidad de las operaciones bancarias electrónicas, establecer criterios de interpretación judicial sobre la responsabilidad de las instituciones bancarias por fraudes cibernéticos puede transformarse en una madeja difícil de desenvolver.

En su tarea decisoria, ciertamente compleja, a los magistrados les toca resolver reclamos llegados a los tribunales en los cuales deben ponderar los aspectos centrales de la problemática de cara a las características del caso concreto para dictar una solución justa y equilibrada. Esto requiere que los intérpretes lleven a cabo un análisis que debe trascender lo meramente dogmático y exige considerar las implicancias sociales y económicas de los fallos que dicten.

Con respecto a lo anterior, es preciso adelantar que la elucidación de estas cuestiones, en consonancia con los principios fundamentales del derecho de daños, del derecho de los consumidores, de la regulación administrativa de la actividad y del análisis de diversos aspectos vinculados a la tecnología bancaria, constituye un imperativo ineludible para contribuir a mejorar el derecho y, por consiguiente, la sociedad. La coexistencia de reglas y principios aplicables en tales supuestos requiere, por lo tanto, de un imprescindible diálogo de fuentes.

En este contexto, la cuestión central que aborda esta investigación es la siguiente: ¿Qué tipo de responsabilidad corresponde atribuir a los bancos cuando sus clientes, al utilizar los servicios en línea ofrecidos por estas entidades, son víctimas de delitos informáticos llevados a cabo por terceros?

En este trabajo se realiza un análisis dogmático para examinar la problemática teniendo en cuenta la legislación aplicable y las particularidades que asume la cuestión respecto del derecho de daños en el actual sistema de fuentes del ordenamiento, revisando diferentes aspectos que se consideran relevantes para comprender cabalmente el objeto de estudio. Para cumplir ese propósito se determinan los objetivos de la investigación.

Objetivos

Objetivo General

Determinar el alcance y fundamento jurídico de la responsabilidad civil bancaria frente a los daños causados a sus clientes por ilícitos informáticos.

Objetivos Específicos

• Analizar el derecho aplicable y los criterios jurisprudenciales pronunciados respecto de la responsabilidad de los bancos por daños causados a sus clientes por ilícitos informáticos.

• Indagar sobre el alcance de las medidas de seguridad que deben adoptar los bancos al emplear herramientas tecnológicas en los servicios ofrecidos a sus clientes para prevenir el fraude informático.

• Conocer el alcance de la tutela que brinda la Ley de Protección del Consumidor a los usuarios de servicios financieros damnificados por ilícitos informáticos.

• Comparar los criterios adoptados por los Tribunales al determinar la responsabilidad de las instituciones bancarias por daños causados a sus clientes por ilícitos informáticos.

Hipótesis

Las entidades bancarias responden en forma objetiva por los daños causados a los consumidores de sus servicios cometidos por terceros utilizando medios informáticos.

Tipo y Diseño de Investigación

En relación a su finalidad, es una investigación básica o pura, de naturaleza dogmática y enfoque cualitativo. Adopta un diseño no experimental, transversal y de carácter bibliográfico, eligiendo como técnica la observación de documentos con el propósito de recopilar, seleccionar y clasificar datos relevantes de acuerdo a los objetivos formulados.

El trabajo tiene enfoque cualitativo, e indaga en la dinámica que presenta la institución examinada a fin de interpretarla; Su nivel de análisis es descriptivo: busca precisar con claridad su objeto de estudio para exponer sus caracteres esenciales, o –en palabras de

Danhke (citado en Hernández Sampieri et al. 2014, p. 60)- “especificar las propiedades importantes” del fenómeno, que se estiman pertinentes para su adecuada comprensión.

La información recolectada se analiza mediante la hermenéutica jurídica; para comprender los textos jurídicos y determinar su sentido. A fines de interpretar los datos se utilizan técnicas de análisis crítico, determinando los contenidos esenciales de las fuentes consultadas; para examinar el contenido de las posiciones jurisprudenciales se emplea el resumen analítico. A partir de la información obtenida se expresan las conclusiones de la investigación, para después formular las propuestas consideradas oportunas.

Se adopta una metodología de carácter documental con diseño bibliográfico, utilizando la observación de los documentos como técnica para la recopilación, selección y clasificación de los datos. Para su recolección se emplea la técnica del fichaje, registrando en hojas de datos la información más relevante.

Se analiza la información para determinar el alcance y fundamento de la problemática de investigación, describiendo el marco jurídico previsto en la actualidad por el ordenamiento vigente y los criterios esgrimidos por los tribunales al respecto. Las fuentes de información proporcionan la materia prima indispensable para ello. A tal fin, se revisan documentos que contienen comentarios, críticas y antecedentes de las normas jurídicas en estudio, debidamente actualizadas. Específicamente, se consultaron las siguientes:

- Normativa aplicable al problema de investigación (Constitución nacional, Código Civil y Comercial, Ley del Consumidor y leyes especiales).
- Publicaciones doctrinarias dedicadas al tema.
- Jurisprudencia relevante de tribunales nacionales y provinciales
- Decisiones administrativas pertinentes (Comunicaciones del BCRA)

El análisis de datos comprende, en consecuencia, el examen de las normas legales aplicables, de la doctrina desarrollada en torno a la cuestión y de la jurisprudencia más

relevante, tanto provincial como nacional, para llegar a descubrir los aspectos principales acerca de la problemática bajo análisis. Se determina en particular el período 2008-2023 como recorte temporal para efectuar el rastreo histórico de las decisiones judiciales revisadas, estableciendo la selección según su pertinencia e importancia para el estudio del tópico.

La investigación desarrolla su contenido en 5 capítulos, de la siguiente manera:

En el Capítulo I se revisa de manera sintética la organización y estructura del Sistema Bancario Argentino, la importancia y naturaleza de la actividad bancaria en la actualidad, la evolución que ha experimentado en el marco de la Revolución 4.0 y las medidas de ciberseguridad que debe adoptar el sector bancario para prevenir la comisión de ciberdelitos de acuerdo a la normativa regulatoria vigente. Luego, se revisan las medidas implementadas por los bancos para evitar fraudes cibernéticos en perjuicio de los usuarios.

El Capítulo II repasa las principales modalidades de ilícitos informáticos, en virtud de su importancia para el examen de la responsabilidad de los bancos frente a sus clientes por los daños sufridos.

En el Capítulo III se examina el tipo de relación jurídica que se establece entre las entidades bancarias y los usuarios a partir de la intersección entre la normativa civil y comercial, la regulatoria del sector financiero y el derecho de los consumidores.

El capítulo IV analiza la responsabilidad de los bancos por la comisión de fraudes cibernéticos en perjuicio de sus clientes, así como el rol que juega la eventual negligencia de los mismos como eximente en tales casos. Además, se examinan en forma comparativa las posturas adoptadas por los tribunales para determinar el alcance y los límites de la responsabilidad bancaria en los casos jurisprudenciales más relevantes a fin de identificar y comparar los patrones, estándares y criterios aplicados por los tribunales para determinar la responsabilidad de los bancos en los supuestos mencionados

Por último, en el apartado final se exponen las conclusiones de la investigación a la luz de los aspectos teóricos y empíricos analizados en torno a la problemática de estudio.

En vista de lo expuesto, el estudio pretende ofrecer una visión integral y actualizada de las implicancias jurídicas que surgen de los ilícitos informáticos en el ámbito bancario, buscando generar aportes para el desarrollo de un criterio jurídico claro y consistente que proteja de manera adecuada a los clientes de los bancos en tanto consumidores y establezca la extensión y límites de la responsabilidad de las entidades bancarias.

Se espera realizar un aporte a la consolidación de un sistema jurídico que contemple la evolución y dinamismo de la tecnología en beneficio del sistema de crédito y, al mismo tiempo, fortalezca la seguridad de las relaciones entre consumidores y bancos en el contexto de la sociedad actual.

Capítulo I

El Sistema Bancario Argentino, su Regulación y la Revolución 4.0

El sistema financiero desempeña un papel vital en una economía de mercado, especialmente con los recientes avances tecnológicos adoptados en el sector, que han permitido a los bancos llegar a más personas y facilitar la comunicación con sus clientes, así como ofrecer canales alternativos para realizar diversas operaciones. Este crecimiento se ha extendido a muchos sectores de la economía formal que anteriormente no estaban incluidos en la cartera de usuarios de la banca, como algunos trabajadores asalariados y los jubilados.

En la actualidad, el sistema financiero se integra por dos tipos de mercados, por intermedio de los que se movilizan y canalizan recursos financieros en la economía: por un lado, el mercado monetario o bancario, regulado por Ley 21526 de Entidades Financieras, y por el otro, al mercado de capitales o de valores, que se rige por Ley 26831 de Mercado de Capitales. Estos ámbitos presentan “segmentos normativos bien diferenciados en cuanto a su

estructura, funcionalidad, agentes operativos e instrumentos financieros transables" (Barreira Delfino, 2011, pág. 173)

En lo que respecta en particular al sistema bancario, su función principal es intermediar entre los agentes económicos que disponen de excedentes de fondos y aquellos que precisan de financiamiento para desarrollar actividades productivas o de consumo. Los bancos son, las entidades que captan recursos en forma de depósitos de unos agentes y conceden préstamos a otros, facilitando de ese modo el flujo de recursos en la economía.

El sistema bancario en Argentina está compuesto por diferentes entidades financieras que ofrecen una amplia variedad de servicios a sus clientes. Los agentes investidos y autorizados para intermediar en la oferta y demanda de recursos financieros se encuentran taxativamente enumerados en la Ley 21526, que menciona, entre otros, a los bancos comerciales, instituciones más conocidas del sector, que ofrecen servicios como cuentas corrientes, tarjetas de crédito, préstamos y depósitos a plazo fijo.

Se ha señalado (Barreira Delfino, 2011) que existe una doble esfera de financiamiento en el ámbito bancario: en una parte se encuentra el de la "banca individual, personal o de consumo" y en la otra, el de la "banca comercial, empresarial o corporativa". Esa bifurcación es visible por el vínculo establecido con la clientela de cada uno de esos sectores, en especial "desde la defensa del cliente bancario o consumidor financiero, tutela de raigambre constitucional a partir de la reforma introducida a la Carta Magna en el año 1994 (art. 42º de la Constitución Nacional)" (Barreira Delfino, 2011, p. 173).

El funcionamiento del sistema bancario tiene un impacto directo en el crecimiento económico y en la estabilidad financiera, siendo un elemento clave en la economía del país, al estar encargado de canalizar los recursos financieros hacia distintos sectores productivos. Asimismo, ocupa un rol importante en la gestión de los riesgos financieros, como el riesgo de

crédito o el riesgo de mercado. Esos riesgos pueden surgir en el marco de las Infraestructuras de los Mercados Financieros (FMI, por sus siglas en inglés), acerca de las cuales se dice que:

> Las infraestructuras de los mercados financieros (FMI) que permiten la compensación, la liquidación y el registro de operaciones monetarias y otras operaciones financieras pueden fortalecer los mercados a los que prestan servicios y desempeñar una función fundamental en el fomento de la estabilidad financiera. No obstante, si no se gestionan adecuadamente, pueden generar riesgos importantes para el sistema financiero y ser una posible fuente de contagio, especialmente en periodos de tensión en el mercado (CPSS-IOSCO, 2012).

En consecuencia, el sistema debe estar bien estructurado y regulado para garantizar su eficiencia y estabilidad y contribuir al desarrollo económico. Por tal razón, la actividad del sector está sometida a regulaciones y controles estrictos, establecidos principalmente por la Ley de Entidades Financieras (LEF), que desde 1977 regula la actividad de los bancos.

La LEF encarga la supervisión y el control de todas las entidades que forman parte del sistema bancario al Banco Central de la República Argentina (BCRA). entidad autárquica responsable de mantener la estabilidad monetaria y financiera del país, emitir la moneda nacional, administrar las reservas internacionales, promover el desarrollo económico y proteger los intereses de los usuarios y consumidores financieros.

En la Carta Orgánica (CO) del BCRA (Ley N° 24.144) se establece la organización interna del organismo y los poderes y funciones a su cargo para vigilar la estabilidad del sistema y proteger los intereses de los usuarios, dándole la potestad de emitir las regulaciones financieras pertinentes y controlar su cumplimiento. Para ello, el BCRA trabaja en estrecha colaboración con otros organismos reguladores y supervisores, como la Comisión Nacional de Valores (CNV) y la Superintendencia de Seguros de la Nación (SSN).

El BCRA se rige por las disposiciones de su CO y demás normas legales concordantes (art.1). Más adelante el art. 4 último párrafo prevé que, en el ejercicio de sus funciones y facultades, no estará sujeto a órdenes, indicaciones o instrucciones del Poder Ejecutivo Nacional (PEN) ni podrá asumir obligaciones de cualquier naturaleza que impliquen condicionarlas, restringirlas o delegarlas sin autorización expresa del Congreso de la Nación".

La condición de entidad autárquica le asegura la máxima independencia de la que un ente estatal puede gozar según el derecho administrativo, al menos técnicamente. Una entidad autárquica es toda persona jurídica pública considerada como órgano estatal que: 1°) es de administración indirecta del Estado y obra en la administración en virtud de un derecho subjetivo y dentro de sus límites; 2°) no está subordinada jerárquicamente a ningún otro órgano administrativo, pues sus atribuciones derivan directamente de la ley y no de un superior jerárquico (Marienhoff, 1987).

El BCRA es responsable de toda trasgresión legal, pudiendo ser demandado a causa de sus actos y demandar en defensa de sus derechos. Todas las acciones que desarrolla influyen de modo directo o indirecto sobre las entidades del sector, generando entre ambas, relaciones jurídicas-legales. La causa de tales relaciones se encuentra en la potestad administrativa delegada por la ley al BCRA, enunciada de modo genérico como “poder de policía financiero”: potestad de reglamentar esta actividad conforme a las leyes generales, ejercer la vigilancia y aplicación de esas normas y aplicar sanciones a la transgresión de su régimen específico (Marienhoff, 1987).

En el cometido de vigilar el buen funcionamiento del mercado financiero y aplicar la LEF y normas concordantes, se genera un contacto jurídico natural con las entidades financieras, y en grado sucesivo con sus clientes, de modo que un comportamiento apartado de las pautas legales que rigen su obrar puede verificarse no solo respecto de los bancos que controla sino también sobre la clientela de estos en cuanto resulte igualmente damnificada:

- Frente a situaciones regulares: aunque los bancos ejecutaran comportamientos disvaliosos inadvertidos por el BCRA., incluso si fueren irregulares desde un punto de vista estrictamente jurídico, ello no implicaría necesariamente que la entidad transgresora no pueda responder patrimonialmente por los daños que ocasione. De tal forma, aunque exista responsabilidad del BCRA por su acción u omisión, será en primer lugar el propio banco que cause el daño quien deba responder; a menos que hubiera obrado conforme le impusiera la autoridad de aplicación, y pueda atribuir a esta la responsabilidad de su obrar.
- Frente a situaciones de crisis, y ante la disminución de la capacidad de responder por parte de la entidad afectada, se presume la responsabilidad de la autoridad de aplicación, en tanto es a esta a quien la ley le impone detectar, evitar y sanear la crisis de las entidades financieras. Por ende, si no se detecta, corrige o neutraliza, hay evidencia de una actuación insuficiente del BCRA. (Toscano, 2006).

La actividad regulatoria de la entidad viene cobrando una importancia aún mayor a causa del proceso de digitalización experimentado en los últimos decenios y acentuado desde principios de este siglo. En este período se han producido cambios importantes, ya que la humanidad ha dejado de ser una sociedad industrial para convertirse en una sociedad posindustrial, proceso denominado “Revolución 4.0”, y caracterizado por el surgimiento de tecnologías disruptivas.

La tecnología informática, que amalgama el procesamiento de datos, la electrónica y el software, ha dado impulso a una transformación profunda en la sociedad. Esta revolución ha desencadenado un amplio abanico de oportunidades en los ámbitos comerciales, sociales y culturales, alterando fundamentalmente los paradigmas de comunicación, así como las concepciones de tiempo y espacio. Simultáneamente, la tecnología de la información ha sido

catalizada por el surgimiento de factores concomitantes, como la proliferación masiva de operaciones y la metamorfosis del concepto de consumo (Farinati, 2009).

La evolución informática y el incremento de la comunicación y la información a escala global ha producido una transformación sustancial en la forma de operar del sector bancario, modificando de manera notoria la relación entre las entidades y sus clientes. Una de las consecuencias más notables de esos cambios ha sido la progresiva sustitución de la prestación del servicio bancario en forma personal por el uso de la tecnología electrónica que permite operar a distancia. El desarrollo de los sistemas informáticos fue reemplazando el trabajo humano dentro de los bancos y cambiando las formas de atender a los clientes, con quienes se tiene menor contacto personal, lo que genera que las operaciones bancarias se realicen más fácilmente y con mayor velocidad (Toscano, 2006).

La transformación experimentada en la operatoria de la banca permite apreciar la creciente importancia de los canales o medios electrónicos en el desarrollo de los servicios bancarios. Las formas tradicionales para operar con los clientes van entrando en desuso, e incluso surgen cada vez más entidades que, enmarcadas en el ámbito de la denominada "banca virtual pura", brindan sus servicios únicamente mediante canales electrónicos (Farinati, 2009).

Esta realidad en permanente transformación ha requerido, lógicamente, de nuevas respuestas por parte del ordenamiento jurídico. Por ejemplo, el uso creciente de los canales electrónicos en la instrumentación de las operaciones bancarias ha traído como inevitable corolario la necesidad de establecer normas, estándares y medidas orientadas a otorgar seguridad material y jurídica a los usuarios del sistema.

Actividad Bancaria y Riesgo Operacional

La actividad bancaria ha sido caracterizada como una práctica esencial e inherentemente riesgosa, además de sumamente vulnerable teniendo presente su alto nivel de

endeudamiento. Ese riesgo juega en esta actividad como un acicate, pues a mayor riesgo es mayor la rentabilidad, siendo difícil conocer la exacta dimensión del riesgo a asumir. "[…] allí radica, precisamente, la virtud del buen banquero" (Villegas, 2005, p. 56).

Para Malvaso (2017) prácticamente toda la actividad bancaria (la intermediación financiera, así como actividades de cambio y diversos tipos de servicios) está expuesta a distintas clases de riesgos, que se clasifican en (Malvaso, 2017; Camerini, 2012):

- Riesgos de Crédito
- Riesgo de Mercado
- Riesgos de Liquidez
- Riesgo Operacional

Este último (Riesgo Operacional -RO) se relaciona directamente con los productos y servicios ofrecidos por vía electrónica. El RO es uno de los factores que representa mayores pérdidas monetarias para los bancos, está asociado con todas las actividades, productos, sistemas y procesos y tiene orígenes muy diversos (procesos, fraudes internos y externos, tecnológicos, recursos humanos, prácticas comerciales, desastres, proveedores). (González & Solís, 2012).

Aunque no existe consenso en torno a la definición de RO, como sí ocurre con respecto a los otros riesgos mencionados, tiene gran aceptación la formulada por el Comité de Supervisión Bancaria de Basilea (BCBS). Para ese organismo, el término genérico RO comprende el riesgo de pérdida originado en la inadecuación o fallas en los procesos, en el personal y en los sistemas internos, o bien, a causa de acontecimientos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y el de reputación (BCBS, 2004: 137).

El riesgo legal incluye, entre otros, la posibilidad de ser sancionado, multado u obligado a pagar daños punitivos como resultado de acciones supervisoras o de acuerdos

privados entre las partes. El riesgo estratégico (abarca los riesgos político, impositivo y regulatorio) y de reputación en general no se incluyen para determinar la exigencia de capital por RO (BCBS, 2004, p. 137).

El fenómeno de la globalización de los mercados y la aparición de productos y servicios tecnológicos como la banca electrónica no han intensificado la complejidad de las actividades empresariales y contribuido, además, a incrementar la exposición de las empresas al RO. El sector financiero debe enfrentar los mayores desafíos en este contexto, debido a su objeto social y a las características de la actividad que desarrolla. En vista de la amenaza que representa para la industria financiera, las entidades del sector están obligadas a gestionar el RO aplicando medidas oportunas y eficaces para disminuir su vulnerabilidad.

En tal sentido, el BCBS advirtió en 2003 que las actividades bancarias son cada vez más complejas principalmente por la creciente sofisticación de las tecnologías utilizadas. Señaló, además, factores involucrados en ese proceso como la expansión del comercio electrónico, la automatización de las operaciones y la mayor integración de tecnologías informáticas y servicios compartidos entre entidades. Por último, estableció en cabeza de los bancos la obligación de identificar y evaluar el RO inherente a todos sus productos, actividades, procesos y sistemas relevantes (BCBS, 2004).

La tecnología es uno de los elementos que integra el RO, y los bancos deben vigilar celosamente el entorno de ciberseguridad de sus operaciones En la actividad bancaria, los sistemas implementados para el desarrollo de operaciones electrónicas o cibernéticas están expuestos a riesgos. En ese marco, los ciberataques son los que generan más preocupación al sector bancario, aprovechando la vulnerabilidad de los sistemas dispuestos para operar.

Esa vulnerabilidad emerge con claridad cuando una deficiente gestión del RO viene acompañada de la implementación de sistemas operativos obsoletos y la omisión en implementar protocolos robustos de ciberseguridad. Asimismo, la falta de medidas de

protección puede constituir un caldo de cultivo propicio para que los ciberdelincuentes vulneren la integridad del entorno operativo, comprometiendo de ese modo la seguridad de la información y de las transacciones. En virtud de estas contingencias, los bancos se hallan expuestos a potenciales consecuencias indeseadas, como las siguientes:

- Pérdida o divulgación de datos/información de la propia organización.
- Pérdida o divulgación de datos/información de sus clientes.
- Pérdida o divulgación de datos/información de sus proveedores.
- Reclamos de clientes.
- Reclamos de Asociaciones de consumidores.
- Robo de valores.
- Interrupción de la Red/interrupción del Negocio.

Adicionalmente, la falta de diligencia en salvaguardar activos, datos y sistemas puede causar perjuicios significativos en la credibilidad, reputación y prestigio de las entidades. En última instancia, puede erosionar la confianza depositada en los bancos por su cartera de clientes, basada en la garantía de seguridad y solidez inherente a la actividad financiera. (Malvaso, 2017).

El Banco Central y la Protección de los Usuarios Financieros

En el art. 4 inc. h de la CO del BCRA se establece que es competencia de esa entidad, el "… Proveer a la protección de los derechos de los usuarios de servicios financieros y a la defensa de la competencia, coordinando su actuación con las autoridades públicas competentes[2] en estas cuestiones…". El Directorio del BCRA se encarga de dictar las

[2] El art. 41 LCD establece las autoridades de aplicación en el orden nacional (Secretaría de Comercio Interior u organismo que la sustituya) y local (gobiernos provinciales y de la ciudad de Buenos Aires). El art. 42 LCD declara que tales competencias son concurrentes. Además, el art 45 LCD último párrafo establece que la ciudad de Buenos Aires y las provincias "…dictarán las normas referidas a su actuación como autoridades de aplicación, estableciendo en sus respectivos ámbitos un procedimiento compatible con sus ordenamientos locales.".

reglamentaciones correspondientes, vinculadas con las que regulan las relaciones entre entidades financieras y clientes que revistan la condición de consumidores. En otras palabras, dicho órgano tiene a su cargo adoptar medidas para proteger los derechos de los clientes financieros, siempre que sean “consumidores o usuarios”, en los términos de la LDC.

Las normas de protección de los usuarios financieros definen específicamente el universo de personas a las cuales se aplicarán, fuera del cual la relación no será considerada como una de consumo en los términos del art 3 LDC en conjunto con los arts. 1 y 2 LCD y la remisión implícita contenida en el art 4 inc ‘h’ de la CO En el art. 36 LDC se definen los requisitos de los documentos de las operaciones financieras para consumo y de los de crédito para consumo y se encomienda al BCRA adoptar “…las medidas conducentes para que las entidades sometidas a su jurisdicción cumplan, en las operaciones a que refiere el presente artículo, con lo indicado en la presente ley…”.(BCRA, 2022).

La normativa busca proteger a aquellas personas que utilizan los productos y servicios que ofrecen las entidades y cuyo vínculo refleja una desigualdad de información y recursos entre quien vende/brinda el servicio y quien lo adquiere/recibe. En ese contexto, se considera USF a las personas humanas y jurídicas que en beneficio propio o de su grupo familiar o social y en carácter de destinatarios finales hacen uso de los productos y servicios ofrecidos por los bancos, compañías financieras, tarjetas de crédito o proveedores no financieros de crédito, sin utilizarlos para su actividad comercial. Por lo tanto, quienes hagan uso de servicios financieros como parte de su actividad comercial, no se consideran “usuarios/as de servicios financieros”. (BCRA, 2022).

La superintendencia que ejerce el BCRA sobre las entidades financieras y cambiarias de la Argentina se lleva adelante por medio de diferentes métodos, en primer lugar, por autorizaciones que deben requerir las entidades al BCRA para su funcionamiento, además en forma periódica los bancos y entidades financieras deben informar una cantidad de cuestiones

operativas al BCRA, también deben seguir determinados resguardos que hacen a su solvencia económica y técnica, y por supuesto, respetar toda la normativa de información que se refiere a la relación que tienen con sus clientes-usuarios. (Malvaso, 2017, Villegas, 2005).

Las entidades alcanzadas son:

- Bancos y compañías financieras
- Emisoras tarjetas de crédito
- Operadores de cambio
- Otros proveedores no financieros de créditos
- Fideicomisos financieros

Además, desde el 1 de marzo de 2023 se incorporaron otros sujetos obligados:

- Proveedores de servicios de pago que ofrecen cuentas de pago
- Proveedores de servicios de pago que cumplen la función de iniciación (PSI) y prestan el servicio de billetera digital (BCRA, 2022).

El BCRA precisó, asimismo, que existen 531 entidades que deben cumplir con la normativa de PUSF, estando reguladas y monitoreadas en lo concerniente a su obligación de protección. En general, se distinguen los siguientes sujetos obligados:

- Todas las entidades financieras (Bancos y Compañías Financieras) que brindan servicios a personas físicas sin actividad comercial
- Las emisoras de tarjetas de crédito y/o compra
- Los operadores de cambio
- Otros proveedores no financieros de créditos ─incorporados recientemente─ y
- Los fideicomisos financieros (BCRA, 2022).

En el marco de los avances tecnológicos, la diversidad de participantes del sistema financiero y sus interconexiones, y la expansión de los servicios financieros digitales, el

BCRA inició el camino para abordar los riesgos y amenazas asociados mediante la adopción de buenas prácticas y lineamientos en 2020 y 2021. En particular, adoptó:

Lineamientos de Ciberseguridad y Ciberresiliencia y Glosario de Ciberseguridad - 2020.

Guía de autodiagnóstico sobre implementación de los lineamientos - 2021.

Lineamientos de Respuesta y Recuperación de ciberincidentes - 2021. (BCRA, 2022).

En esa línea, el BCRA publicó disposiciones dirigidas a las entidades: la Comunicación A 7072, impone que implementen recaudos especiales antes de efectivizar una transferencia para minimizar el riesgo, particularmente respecto a cuentas de destino que: a) no hayan sido previamente asociadas por el originante; b) no registren una antigüedad mayor de 180 días desde su apertura; c) no hayan registrado depósitos o extracciones en los 180 días anteriores a la fecha en que sea ordenada la transferencia inmediata. En tanto, la Comunicación A 7175, exige ofrecer y utilizar en la operatoria con sus clientes herramientas de mitigación de fraude para identificar patrones sospechosos y alertar a los usuarios.

Luego, en la Comunicación A7266, el BCRA estableció lineamientos para la respuesta y recuperación ante ciberincidentes con el fin de limitar los riesgos en la estabilidad financiera e impulsar la ciberresiliencia del ecosistema en conjunto, en línea con las recomendaciones del Consejo de Estabilidad Financiera (FSB, por sus siglas en inglés), Estos lineamientos están dirigidos a entidades financieras, proveedores de servicios de pago que ofrecen cuentas de pago e infraestructuras del mercado financiero, pero por su carácter general, pueden ser adoptados por cualquier institución del sistema financiero.

Un ciberincidente, según la definición incluida en el glosario publicado en la página web del BCRA (ver Anexo), es un evento relacionado a una infraestructura tecnológica en la que interactúan personas, procesos, datos y sistemas de información y que pone en peligro la

ciberseguridad o infringe las políticas o procedimientos de seguridad o las políticas de uso aceptables por las entidades, sea o no un evento producto de una actividad maliciosa.

Respecto a su ejecución, los actores alcanzados podrán adoptar las prácticas más adecuadas para sus modelos de negocio, teniendo en cuenta su tamaño, complejidad o riesgos en relación con el ecosistema financiero. Deberán dejar constancia de los fundamentos de los criterios adoptados y ponerlos a disposición de la Superintendencia de Entidades Financieras y Cambiarias cuando se les solicite. La Comunicación presenta las siguientes directrices:

1. Gobierno: Se propone establecer un marco de decisiones que involucre a participantes internos y externos en la coordinación y gestión de ciberincidentes, fomentando una cultura proactiva de respuesta.
2. Planificación y Preparación: Se destaca la importancia de la preparación previa para una respuesta y recuperación efectivas. Los planes y procedimientos, con criterios para activar medidas y responder ante ciberincidentes, juegan un rol crucial.
3. Análisis: Implica el análisis forense, la evaluación del impacto y la investigación de la causa. Se sugiere la creación de una taxonomía para clasificar los ciberincidentes.
4. Mitigación: Enfoca en medidas para prevenir el agravamiento y erradicar consecuencias de ciberincidentes, incluyendo contención, aislamiento y erradicación.
5. Restauración y Recuperación: Detalla la restauración de sistemas, activos y datos afectados por ciberincidentes, buscando la normalidad de operaciones y servicios.
6. Coordinación y Comunicación: Subraya la importancia de coordinar con actores internos y externos, y establecer comunicación eficaz y adaptada al público destinatario.
7. Mejora Continua: Hace hincapié en la incorporación de lecciones aprendidas en casos anteriores y el uso de herramientas proactivas, como ejercicios, pruebas y simulacros, para fortalecer las capacidades de respuesta y recuperación.

Más tarde, en la Comunicación “A” 7319 del 1 de julio de 2021, el BCRA estableció que para autorizar un crédito pre aprobado la entidad debe verificar fehacientemente la identidad de la persona usuaria involucrada, entre otras medidas. Esta comunicación reconoce como antecedente el procedimiento *Conozca a su Cliente*, recomendación del Comité de Basilea conforme a la cual los bancos deben establecer un conjunto de reglas y procedimientos bien definidos para identificar la identidad y determinar el origen y constitución del capital y recursos financieros del cliente o usuario.

Posteriormente, a fin de fortalecer la ciberresiliencia de las entidades que proveen servicios financieros y brindar mayor seguridad a sus usuarios, el BCRA publicó en marzo de 2023 la Comunicación A 7724 que actualizó los “Requisitos mínimos para la gestión y control de los riesgos de tecnología y seguridad de la información”, obligando a las entidades financieras a implementar un sistema de control interno y de gestión de riesgos en tecnología y seguridad de la información en sus operaciones cibernéticas. Reformuló las reglas que regían anteriormente (Comunicación A 4609 y sus modificatorias) y, si bien mantiene gran parte de sus aspectos técnicos, profundiza el fortalecimiento de la estructura de gobernanza de los sistemas de información. En el sitio web de la entidad se dice que:

> Es una actualización normativa integral, en línea con las recomendaciones internacionales del BIS y del FSB, que establece parámetros mínimos para las entidades financieras en términos del gobierno, la gestión de los riesgos de la tecnología y seguridad de la información, la continuidad del negocio, la tecnología, la infraestructura informática, la gestión de ciberincidentes y aspectos clave para mejorar la ciberresiliencia del sistema financiero (BCRA, 2023).

Esta comunicación alcanza a las entidades financieras y apunta a fijar el conjunto de requisitos mínimos aplicables a los procesos, estructuras y activos de información normativa;

en consecuencia, obliga a esas entidades a realizar una planificación estratégica en materia de ciberseguridad, estableciendo pautas a implementar. Las más relevantes son las siguientes:

1. Doble autenticación

Las entidades están obligadas a definir modelos de acceso para los usuarios que contemplen los factores de autenticación, el comportamiento observado en el uso de servicios y diversas fuentes de información que permitan validar la identidad de los usuarios.

2. Protección de integridad

Deben establecer medidas de protección que aseguren al cliente la integridad y confidencialidad de los factores de autenticación utilizados y reduzcan el riesgo de ataques a través de métodos que prueben la posesión y el control del usuario sobre el dispositivo.

3. Datos biométricos

Se deberán evaluar y mitigar los riesgos sobre las propias limitaciones del método, la tasa de falsos positivos, las posibles vulnerabilidades en los dispositivos y sistemas utilizados para la captura y validación de las credenciales y el impacto en la privacidad de los usuarios.

4. Eventos de seguridad

Tendrán que establecer un proceso para el registro y el análisis de la información relacionada con eventos de seguridad de los sistemas, las redes y la infraestructura tecnológica. Además, deberán revisar los perfiles de comportamiento de los usuarios que permitan identificar sus actividades habituales, y detectar patrones de actividad sospechosa o inusual por parte de los usuarios.

5. Gestión de ciberincidentes

Se deberá realizar un registro del seguimiento de las actividades hasta la identificación de la causa raíz de los ciberincidentes, para asegurar que sean resueltos y no ocurran nuevamente. Cuando no se pueda identificar el origen del ciberincidente, o el mismo no se encuentre bajo control del banco, igualmente habrá que llevar a cabo acciones para

gestionar su seguimiento. Además, las entidades tendrán que analizar la información disponible a fin de prevenir nuevos ciberincidentes, o para investigar la causa raíz del ciberincidente registrado.

6. Cajeros y homebanking

El BCRA considera a cajeros automáticos, banca telefónica, terminales de autoservicio, banca móvil, banda por internet y plataforma de pagos móviles, como elementos comprendidos en los Canales Electrónicos. La Comunicación A 7724 exige a las entidades organizar equipos de trabajo especializados en la gestión de incidentes de seguridad y disponerlos en todos sus Canales Electrónicos.

Recientemente, en junio de 2023 el BCRA publicó la comunicación "A" 7783, la cual establece nuevos requisitos mínimos para la gestión y control de los riesgos de tecnología y seguridad de la información asociados a los servicios financieros digitales para las Entidades Financieras y Proveedores de Servicios de Pago (PSP) de Argentina, alineados con lo definido en la comunicación A 7724.

La nueva comunicación deroga la Sección 11 de las normas sobre "Requisitos mínimos para la gestión y control de los riesgos de tecnología y seguridad de la información" del BCRA. Además, extiende su alcance a las infraestructuras del mercado financiero conocidas como Sistemas de Pago de importancia sistémica (Interbanking, Coelsa, Link y Prisma, entre otras) en busca de una mayor cobertura en la gestión de riesgo de las operaciones realizadas por servicios financieros digitales.

Asimismo, en un entorno de transacciones digitales donde la protección de datos es crucial, exige medidas proactivas que abarcan aspectos esenciales como el control y monitoreo de operaciones en línea, vigilancia de riesgos asociados a cuentas no presenciales, autenticación de clientes, protección de datos personales y encriptación robusta para

transacciones seguras, formación específica para operar en forma segura, establecimiento de vías de comunicación 24/7 y mantenimiento de un registro de eventos de seguridad.

Medidas de Seguridad Adoptadas por el Sector Bancario

En el contexto de la significativa transformación digital experimentada en el sector, las entidades bancarias han emprendido algunas medidas con el propósito de resguardar tanto sus activos como la información de sus clientes, sin duda asumiendo que resultan imprescindible para enfrentar los desafíos de la ciberdelincuencia, problemática que se viene presentando desde la llegada de internet, pero que se ha exacerbado notablemente con la propagación de la pandemia de COVID -19.

Dentro del ámbito de la seguridad bancaria, el establecimiento de diversos métodos y procesos efectivos de ciberseguridad es imperativo para asegurar la protección de la información y los activos, a través de la implementación de sistemas de seguridad y canales que difundan actividades de capacitación dirigidas a todos los colaboradores de la entidad.

Uno de los pilares fundamentales de la estrategia de seguridad es la autenticación, que desempeña un papel crucial en la prevención de fraudes. La misma se lleva a cabo mediante diversos medios como tokens, contraseñas o incluso huellas dactilares, para asegurar la confirmación de la identidad de los usuarios antes de permitirles el acceso a los servicios. En un momento posterior a la autenticación, se desarrolla el proceso de autorización, que tiene la finalidad de otorgar a los usuarios la habilitación para acceder a funciones específicas dentro del sistema, como por ejemplo la de realizar transacciones. La implementación de estas medidas de seguridad técnicas es respaldada por su eficacia en la prevención de riesgos.

Algunas medidas que podrían prevenir la ocurrencia de estafas electrónicas Abad (2021) incluyen intensificar las instrucciones algorítmicas para conseguir identificar automáticamente transacciones sospechosas en función de criterios como operaciones de montos inusuales, movimientos atípicos o beneficiarios no registrados. También considera

efectivo mantener un registro de direcciones IP habituales o seguras, lo que permitiría al banco alertar sobre operaciones realizadas desde dispositivos con direcciones IP poco comunes. Agrega, además, que podrían emplearse prácticas que no requieren el uso de tecnología avanzada, señalando que se podrían evitar muchas transacciones fraudulentas si las entidades financieras implementaran medidas como realizar llamadas telefónicas al cliente para confirmar la transacción o exigir que el consumidor se presente en una sucursal física para llevar a cabo ciertas operaciones, como solicitudes de préstamos, por ejemplo.

Entre los ejemplos de medidas implementadas por las entidades del sector dirigidas a fortalecer el entorno de ciberseguridad, se encuentran los siguientes:

El Banco Macro destaca las operaciones digitales en su sector de banca individual, incluyendo la implementación de la tokenización para aumentar la seguridad en los pagos digitales y simplificar las compras de los clientes con tarjetas de crédito y débito en dispositivos móviles y otros. También se menciona la adopción de un motor biométrico propio como medida de seguridad para operar en los canales en línea.

En la memoria anual de Grupo Supervielle (2021) se destacan diversas iniciativas relacionadas con la ciberseguridad, como la implementación de capacidades digitales avanzadas mediante analítica y inteligencia artificial. Además, se hace referencia sobre la migración multicloud para optimizar costos y adaptabilidad, y se resalta la evolución de canales digitales con biometría y atención omnicanal. La introducción de un hub virtual con video asistencia y un nuevo modelo de sucursal virtual también marca un avance en la banca digital. El catálogo de APIs se amplió y se fomenta la innovación en áreas como blockchain y tokenización de activos a través de un entorno de experimentación.

El Banco Patagonia destaca por su liderazgo en información relacionada con la innovación tecnológica y ciberseguridad. Entre sus enfoques relevantes se incluyen el desarrollo de soluciones digitales para mejorar la banca en línea, el acceso a canales de

atención y la experiencia del cliente. También se puede mencionar la implementación de campañas educativas y promocionales sobre el uso de medios electrónicos, así como la realización de capacitaciones sobre seguridad bancaria y protección de datos, enfocada en aspectos esenciales vinculados a la prevención de phishing, el diseño del token online y las prácticas adecuadas en materia de ciberseguridad.

Además, resalta su inversión en equipamiento de última generación con mayor capacidad en los datacenters, así como su compromiso con la regulación al prohibir operaciones con activos digitales no autorizados por el BCRA. Otro aspecto destacable es la implementación de medidas dirigidas a mitigar los riesgos asociados a la operatoria con billeteras digitales.

El informe anual integrado (2021) del Banco BBVA Argentina destaca su enfoque en ciberseguridad y protección de datos, incluyendo la implementación de iniciativas como el desarrollo de un modelo de seguridad y privacidad de datos para el tokenizado de información sensible. En concreto en lo que se refiere a la seguridad de los datos de los clientes, se detalla que durante el 2021 se llevaron adelante diversas iniciativas dentro del portfolio de seguridad y protección de datos para prevenir situaciones fraudulentas en perjuicio de los clientes.

Una de las iniciativas más auspiciosas en lo relativo a las medidas de seguridad implementadas por los bancos en su operatoria digital para evitar la aparición de fraudes electrónicos es la mencionada por la Defensoría del Pueblo de Santa Fe. Esa oficina refirió que, en septiembre de 2022, en respuesta a numerosas quejas de ciudadanos por estafas virtuales, emitió una resolución instando a entidades bancarias como el Banco de Santa Fe y el Banco Central de la República Argentina (BCRA) a tomar medidas para prevenir dichas estafas. El Banco de Santa Fe, en cumplimiento con la solicitud, implementó medidas como alertas para notificar a los usuarios sobre nuevos dispositivos de acceso, supervisión continua

las 24 horas del día, Apps por módulos con selección de operaciones, control de sitios falsos en buscadores y monitoreo de transacciones. Además, la entidad lanzó una campaña de prevención de fraudes para concientizar a los clientes sobre el uso seguro de canales electrónicos. El Banco informó que estas medidas resultaron en una disminución de casos denunciados por los usuarios.

En otro orden de ideas, el hecho de que la conducta de los propios usuarios también juega un papel importante en el entorno de ciberseguridad, ha llevado a que se produzcan debates respecto del alcance de la responsabilidad de las entidades por los eventuales fraudes cometidos por terceros. Esta responsabilidad se extiende desde brindar educación adecuada a los clientes hasta proveerles las herramientas necesarias para comprender los aspectos de seguridad y amenazas existentes en los canales digitales. Es así como se busca fomentar una conciencia de seguridad entre los usuarios (Defensoría del Pueblo de Santa Fe, 2023).

Por otra parte, es relevante mencionar que. en un esfuerzo conjunto, los actores más prominentes del sector financiero argentino tomaron medidas concretas para fortalecer la seguridad de los usuarios. A través de un acuerdo de cooperación entre varias asociaciones bancarias y la Cámara Argentina Fintech, se busca prevenir y controlar transferencias sospechosas entre cuentas con el objetivo de ofrecer una protección integral a los usuarios y consumidores dentro del ecosistema financiero. Este pacto representa una nueva etapa en la lucha contra el delito financiero, complementando las inversiones en tecnología y las campañas de concientización que las instituciones ya están implementando (iProUP).

Capítulo II

Normativa Argentina Sobre Ciberdelincuencia

La ciberdelincuencia es definida por la ONU (2020) como un “acto que infringe la ley […] que se comete usando las tecnologías de la información y la comunicación (TIC) para atacar las redes, sistemas, datos, sitios web y la tecnología o para facilitar un delito (…). Se

diferencia de los delitos comunes en que «no tiene barreras físicas o geográficas» y se puede cometer con menos esfuerzo y más facilidad y velocidad que los delitos comunes (aunque esto depende del tipo de ciberdelincuencia y del tipo de delito con el que se compare)"

En la actualidad, el país cuenta con un conjunto de leyes y normas relativas al ámbito digital, que abordan cuestiones relacionadas con la Protección de Datos personales, tipificación de conductas practicadas en el ámbito digital, protección de la propiedad intelectual y una ley adicional que aprueba el texto del Convenio de Budapest y dicta las vías para su aplicación.

En particular, el Convenio de Budapest sobre Ciberdelincuencia es un tratado internacional creado en el año 2001 e impulsado por el Consejo de Europa con el objeto de fomentar la cooperación internacional y crear un marco legal uniforme entre las naciones para combatir los delitos informáticos y la actividad criminal en Internet.

Recientemente, el 16 de febrero de 2023 la Argentina firmó la adhesión al Segundo Protocolo Adicional del Convenio de Budapest de la Unión Europa sobre ciberdelitos. El Protocolo mantiene las condiciones y salvaguardas de los derechos fundamentales ya incluidas en el Convenio y sirve como guía para cualquier país que desee desarrollar una legislación nacional integral sobre ciberdelitos y como un marco para la cooperación internacional entre los Estados Parte del Convenio.

La adhesión de Argentina al Convenio de Budapest se llevó a cabo pese a las advertencias realizadas por parte de la sociedad civil y del mundo académico que advertían sobre a la amplitud y ambigüedad de algunas disposiciones abiertas y genéricas contenidas en el texto, también presentes en la Ley 26.388 de delitos informáticos, que favorecen interpretaciones arbitrarias y potenciales abusos por parte de las autoridades (Martins dos Santos, 2022).

Con la sanción de la Ley Nº 27.411 se internalizó en el ordenamiento jurídico argentino las disposiciones del Convenio de Budapest, aunque debe tenerse en cuenta que la adhesión de Argentina se hizo con reservas, ya que algunas de sus disposiciones representaban un conflicto potencial con la legislación nacional. En consecuencia, se dejaron afuera aquellas relacionadas sobre todo a medidas sobre pornografía infantil y otras cuestiones jurisdiccionales.

Dicho tratado fue ratificado el 05 de junio de 2018, y entró en vigor el 1 de octubre de ese año. Las disposiciones más relevantes que regula son las siguientes:

- Estimula la colaboración entre las partes para investigar y proceder en casos de infracciones penales vinculadas a sistemas y datos informáticos, así como para recolectar pruebas electrónicas en estos delitos.
- Se contempla la designación de una o más autoridades centrales para el intercambio de solicitudes de asistencia mutua, su ejecución o su remisión a las entidades competentes, con comunicación directa entre dichas autoridades.
- Facilita la obtención de información sobre registros de nombres de dominio e información de abonado a través de proveedores de servicios en otras jurisdicciones, definiendo proveedores como entidades que ofrecen comunicación por sistemas informáticos.
- En situaciones de urgencia, las autoridades pueden utilizar medios expeditivos como fax o correo electrónico para solicitar asistencia mutua o intercambiar información relacionada.
- Se propicia el empleo de videoconferencias y equipos conjuntos de investigación adaptados a la naturaleza de los ciberdelitos y la prueba electrónica.

Ciberdelitos en el Ámbito Bancario

En la actualidad, la evolución acelerada de la tecnología y la transformación que impulsa en las actividades humanas hace que gran parte de las transacciones, gestiones y tareas individuales y colectivas en el mundo de los negocios dependan cada vez más del uso de Internet y diversas plataformas digitales.

Tanto las personas humanas como las jurídicas, entre ellas las empresas del sector bancario, deben manejar información de todo tipo, empleando sistemas que pueden llegar a ser vulnerables y sufrir ataques o intrusiones. Los bancos, específicamente, manejan una enorme cantidad de información sensible, tanto de sus clientes, como de sus empleados y de la propia entidad, que se administra mediante sistemas y redes de teleprocesamiento de datos.

Los delitos informáticos o ciberdelitos son definidos por Castillo y Ramallo (como son citados por Acurio, 2016) como cualquier acción maliciosa que cause daño a personas o entidades en cuya comisión intervengan dispositivos comúnmente utilizados en actividades informáticas.

Por su parte, según el Ministerio de Justicia y Derechos Humanos (2021) se trata de conductas ilegales realizadas por ciberdelincuentes en el ciberespacio a través de dispositivos electrónicos y redes informáticas. Existe una amplia gama de ilícitos tales como robo de datos personales o de identidad, robo de información comercial estratégica, Phishing y otros fraudes, cometidos por ciberdelincuentes que actúan en grupo o trabajan solos (Ministerio de Justicia y Derechos Humanos, 2021).

Con relación a los ciberdelitos en el ámbito bancario, existen varias modalidades utilizadas para cometer fraude en perjuicio de los usuarios de las entidades. Las más habituales son las siguientes:

Phishing

Es un término informático originado en la contracción de *Password Harvesting Fishing*, denominación del idioma ingles que literalmente significa “cosecha y pesca de

contraseñas" (Borghello y Temperini, 2012) y abarca a los abusos cometidos mediante el empleo de ingeniería social para engañar y obtener de manera fraudulenta información bancaria confidencial de una o más víctimas (Fernández, 2019).

A diferencia de la ingeniería técnica, que está basada en la elaboración de programas maliciosos, la ingeniería social se caracteriza por la implementación de estrategias comunicacionales de manipulación psicológica por parte del ciberdelincuente para ganarse la confianza del usuario elegido como víctima y conseguir que revele información confidencial que le permita realizar un delito posterior. Los delincuentes explotan datos revelados en redes sociales, chats y foros para crear perfiles de usuarios y ejecutar sus engaños (Rodríguez, 2021).

En el Código Penal esta modalidad se encuentra comprendida en el art. 173, inc. 16 (incorporado por Ley 26388) como uno de los tipos de fraude. El delito, denominado "estafa informática", exige para su configuración la existencia del ardid o engaño y del perjuicio patrimonial acaecido a consecuencia de aquél.

En cuanto al modus operandi del Phishing en el sector bancario se desarrolla por lo general cuando sus autores, denominados *phishers*,

> […] simulan pertenecer a entidades bancarias y solicitan a los cibernavegantes los datos de tarjetas de crédito o las claves bancarias, a través de un formulario o un correo electrónico con un enlace que conduzca a una falsa página web […] similar a la original. Si logran engañar al receptor del mensaje obtienen la clave de acceso a sus cuentas y realizan transferencias o retiros de dinero […] (Fernández, 2019, p. 175).

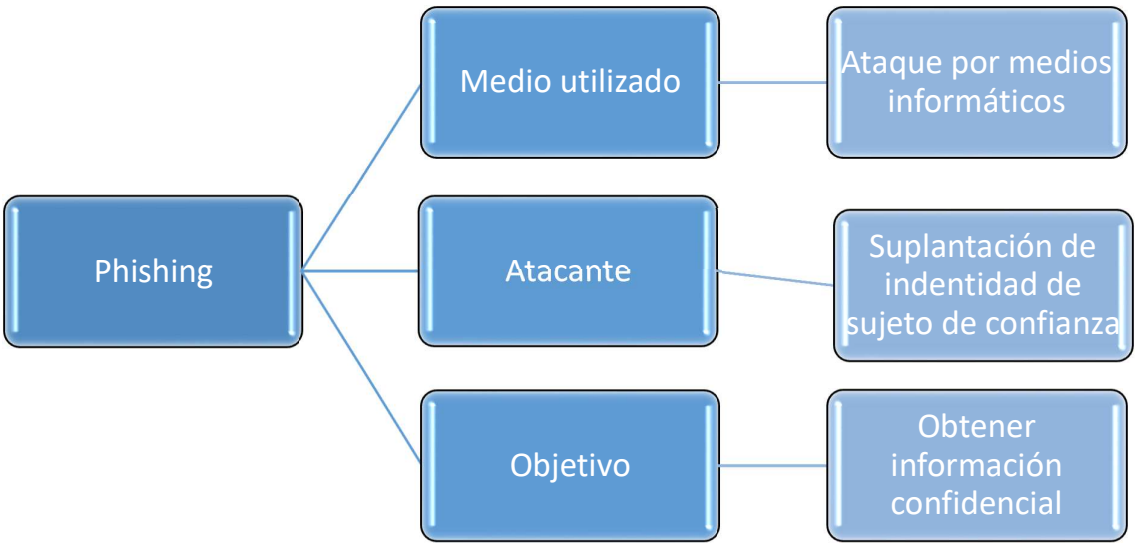

Figura 1. *Esquema Básico del delito de Phishing*

Según el Perito Informático Forense y especialista en Seguridad Pablo Rodríguez (2021), los ataques de Phishing y otros engaños virtuales se han propagado en la Argentina, especialmente durante la Pandemia de Covid-19. Al respecto, destaca el hecho de que, en contra de la creencia común, generalmente los usuarios de internet proporcionan de manera gratuita la información que los ciberdelincuentes utilizan para cometer todo tipo de estafas y engaños.

Pharming

El Pharming es una modalidad de fraude complejo que se aplica en el sector bancario. En este caso la técnica del delincuente consiste en atacar la red y equipos de un usuario para reemplazar el sistema de resolución de nombres de dominio (DNS) a fin de conducir al usuario a una página web bancaria falsa y apoderarse de sus claves. Cuando un usuario teclea una dirección en su navegador, esta debe convertirse a una dirección IP numérica, proceso realizado por los servidores DNS, denominado resolución de nombres. El engaño implica acceder al sistema de un usuario y modificar el sistema de resolución de nombres, de manera

que cuando el usuario crea que entra al sitio de su banco, en realidad ingresa a la IP de un sitio falso (Fernández Delpech, 2014).

Vishing

El vishing es término que provine de la contracción del inglés *phishing by voice* y alude a una modalidad de phishing que se realiza mediante Internet, utilizando números de teléfono IP para simular que son números telefónicos de atención al cliente de entidades financieras. En este tipo de estafa, el usuario recibe un correo electrónico apócrifo que le advierte de una situación relacionada con su cuenta bancaria o de tarjeta de crédito o débito, e incluye un número de teléfono disponible para resolver el problema. Sin embargo, dicho número no corresponde realmente a un servicio telefónico legítimo, sino que está asociado a una cuenta de voz sobre IP, mediante el cual la víctima brinda su clave u otros datos bancarios a los ciberdelincuentes (Arias y Muller, 2021).

Keylogger

Los keylogger son aplicaciones maliciosas o malware de carácter específico tienen como objetivo capturar y almacenar las pulsaciones que se realizan en el teclado conectado a un equipo informático con el propósito de monitorear en todo momento los valores confidenciales introducidos por el usuario. Existen dos tipos de keylogger:

• Por Software: está conformado por el programa informático malicioso que infecta el sistema y envía al atacante la información recolectada.

• Por Hardware: son dispositivos conectados entre el teclado y el equipo que requieren estar ubicados frente a la computadora (Villegas López, 2018).

Capítulo III

Relación Jurídica entre Bancos y Clientes

El análisis de la responsabilidad de los bancos por fraudes electrónicos requiere indagar acerca de las características de la relación jurídica existente entre las entidades bancarias y sus clientes, a fin de examinar qué reglas de interpretación corresponde aplicar a estos casos.

Acerca de la relación jurídica que se establece entre las entidades financieras y los usuarios de sus servicios surgieron distintas posturas; así, en relación al tipo de contrato que celebran las partes de ese negocio jurídico se manifestó primero la doctrina, desde una perspectiva teórica y dogmática, y luego lo hicieron los jueces, obligados por imperativo legal a resolver las diversas disputas sobre distintos aspectos de la problemática.

En torno a la cuestión, el rol del sistema del consumidor es crucial. La sanción en 1993, de la Ley 24.240 de defensa al consumidor tuvo como finalidad principal la protección de los consumidores en todas las etapas de la relación de consumo, aunque no contempló en su articulado la figura del consumidor o usuario de productos o servicios bancarios y financieros. Poco después, en el art. 42 CN, incorporado con la reforma constitucional de 1994, se estableció el marco general de los contratos de consumo:

> *Los consumidores y usuarios de bienes y servicios tienen derecho, en la relación de consumo, a la protección de su salud, seguridad e intereses económicos; a una información adecuada y veraz; a la libertad de elección y a condiciones de trato equitativo y digno. Las autoridades proveerán a la protección de esos derechos, a la educación para el consumo, a la defensa de la competencia contra toda forma de distorsión de los mercados, al control de los monopolios naturales y legales, al de calidad y eficiencia de los servicios públicos, y a la constitución de asociaciones de consumidores y de usuarios. La legislación establecerá procedimientos eficaces para la prevención y solución de conflictos, y los marcos regulatorios de los servicios públicos de competencia nacional, previendo la necesaria participación de las*

asociaciones de consumidores y usuarios y de las provincias interesadas, en los organismos de control.

Esa consagración constitucional tuvo indudable trascendencia para el constituyente y para la ciencia jurídica, ampliando los derechos y garantías de la población. Además, ese reconocimiento de derechos específicos que coexisten con el derecho privado ─aunque lo alteran─ impactó profundamente en el régimen contractual y extracontractual al establecer un doble orden de categorías en las relaciones jurídicas según sean o no de consumo (Tambussi, 2021).

Aunque inicialmente la doctrina y jurisprudencia mayoritarias no admitieron la aplicación de ese sistema a los litigios entre consumidores y entidades financieras, algunos fallos comenzaron a receptar acciones que invocaban la relación de consumo en esos casos. De manera paulatina fue abriéndose paso una corriente favorable a extender la protección de la norma a los consumidores bancarios, criterio que terminó siendo compartido por la mayoría doctrinaria y jurisprudencial

Esa recién fue aceptada con la promulgación de la Ley 26.361, que reformó la LCD y generó un impacto directo en el Sistema Bancario Argentino mediante cambios relevantes tales como ampliar la figura del consumidor a los consumidores y usuarios financieros y bancarios, agregar el concepto de relación de consumo y exigir a los proveedores financieros las formalidades impuestas a los proveedores de bienes y servicios en sus relaciones con usuarios y consumidores

Según resulta del sistema actual adoptado en el CCCN, los contratos bancarios son asimilables a los contratos de consumo en virtud de la relación jurídica que se constituye entre las partes, que buscan satisfacer sus intereses. De tal manera, se perfilan los elementos integrantes del vínculo contractual bancario: por un lado, el subjetivo, integrado por las partes

del contrato, es decir, el banco y su cliente; por el otro, el elemento objetivo, conformado por el crédito.

- Los bancos o entidades financieras: persiguen obtener un beneficio por facilitar recursos dinerarios que reciben y deben prestar.

- Los clientes / consumidores o usuarios: buscan contar con recursos dinerarios para cubrir sus necesidades financieras.

En general, en el artículo 957 del CCyC, se define al contrato como: "(…) el acto jurídico mediante el cual dos o más partes manifiestan su consentimiento para crear, regular modificar, transferir o extinguir relaciones jurídicas patrimoniales". Tal como destaca Rivera (2015), se consagra legislativamente en el texto del Código la noción de contrato anteriormente consensuada por la doctrina y la jurisprudencia en su tarea interpretativa y de aplicación del Código velezano, reafirmando de ese modo el carácter del contrato como todo acto jurídico bilateral y patrimonial.

Por otro lado, en el CCCN se deja establecido de forma expresa que las disposiciones relativas a los contratos bancarios allí previstas se aplican a los contratos celebrados con las entidades comprendidas en la normativa sobre entidades financieras, y con las personas y entidades públicas y privadas no comprendidas expresamente en esa legislación cuando el Banco Central de la República Argentina disponga que tal normativa les resulta aplicable (Art. 1378 CCCN).

Esta prerrogativa reconocida al BCRA es calificada por Mazzinghi (2020) como "polémica", al interpretar que fue concedida a ese organismo en línea con lo previsto en el art. 3° de LEF en tanto dispone que "Las disposiciones de la presente Ley podrán aplicarse a personas y entidades públicas y privadas no comprendidas expresamente en ella, cuando a juicio del Banco Central de la República Argentina lo aconsejen el volumen de sus operaciones y razones de política monetaria y crediticia."

Agrega el autor citado, que el art. 1378 CC tiene un sentido similar a la norma antes transcripta, “aunque en este último caso la propia ley fija una pauta orientadora que limita la discrecionalidad del organismo de control, al prever la posibilidad de ejercer esa potestad cuando “…lo aconsejen el volumen de sus operaciones y razones de política monetaria y crediticia.”. Entiende este autor que un fundamento lógico y medianamente objetivo debe estar configurado para que el BCRA pueda disponer la aplicación analógica de la normativa relativa a contratos bancarios a aquellos contratos que no califiquen técnicamente como tales, ya que lo contrario implicaría convalidar un acto arbitrario y meramente discrecional (Mazzinghi, 2020).

Al respecto, debe temerse presente que las entidades del mercado bancario o crediticio tienen una doble cartera de clientes; por un lado, una cartera con la que se vinculan cuando atraen, administran y canalizan las ofertas y demandas de recursos financieros con destino al financiamiento del consumo de las personas físicas (banca personal); por otro, una cartera con la que se relacionan cuando se ocupan del financiamiento del capital de giro o de trabajo de las empresas (banca empresarial o corporativa). /Barreira Delfino, 2011). Este carácter bifronte ha dado lugar “a la conformación de relaciones jurídicas distintas, con reglas de interpretación también distintas, en especial con relación a la defensa del denominado cliente bancario o consumidor financiero”, en palabras de Barreira Delfino (2011, pág. 173).

Dicha distinción se encuentra plasmada en el criterio establecido por el BCRA cuando ─al regular la actividad de los bancos que prestan servicios en el mercado financiero─ dispone que dichas entidades deben diferenciar a sus clientes entre dos carteras: comerciales o de consumo, El BCRA encuadra en la segunda de esas categorías a los consumidor bancario, a quienes califica como personas humanas o jurídicas que utilizan o adquieren un bien como destinatario final para consumo propio, familiar o social, o aquellas expuestas a una relación de consumo bancaria. Además, incluye en la cartera bancaria de clientes de

consumo a los deudores cedidos entre entidades financieras, estén notificados o no de la cesión. Sin embargo, el BCRA aclara que no forman parte de esa categoría de clientes quienes adquieran servicios bancarios para destinarlos a sus actividades comerciales.

Tal como señala Ritto (2016) con la incorporación de los contratos bancarios al CCCN se establecen principios mínimos que conforman un núcleo duro de tutela pasible de ser ampliado por la legislación especial, tales como la LDC y las Comunicaciones del BCRA. Se prevé, asimismo, la aplicación de la tutela establecida para los contratos de consumo (arts. 1093 a 1122) a los contratos entre las entidades bancarias y los consumidores y usuarios de servicios financieros. Ello importa la consagración de una mayor tutela normativa en favor de los usuarios de los productos financieros, que tiene su epicentro en el Código Civil y Comercial.

En tanto, también existe consenso en torno a que la relación de consumo debe definirse "de modo que abarque todas las situaciones en que el sujeto es protegido: antes, durante y después de contratar; cuando actúa individualmente o cuando lo hace colectivamente, siendo la relación de consumo el elemento que decide el ámbito de aplicación del derecho del consumidor, debiendo comprender todas las situaciones posibles" (Lorenzetti, 2003).

Según Lorenzetti (2006, citado en Ritto, 2015), el banco es una institución profesional con un alto nivel de sofisticación en sus productos y servicios, los cuales ofrece masivamente. Esto permite encuadrar a las relaciones que establece con sus clientes en el ámbito profesional, que se distingue por un desnivel cognoscitivo relevante. Los contratos que celebran las entidades bancarias con sus clientes, o contratos bancarios, son negocios jurídicos que tienen por objeto el crédito (Villegas, 1998, citado por Ritto, 2016).

De tal modo, visto desde el derecho del consumidor, el particular vínculo jurídico examinado se integra con elementos objetivos subjetivos y teleológicos que permiten

distinguir a la relación de consumo dentro del género de las obligaciones. Su elemento objetivo abarca los “bienes o servicios de consumo”, Como elementos subjetivos se encuentra, por un lado, al consumidor o usuario (sujeto activo de protección), y por otro lado al de proveedor (sujeto pasivo), El elemento teleológico es el “destino final” a satisfacer con el acto de consumo (Rusconi, 2008).

Bajo el prisma del sistema protectorio del consumidor, la categoría de cliente bancario comprende a los sujetos que tienen una “vinculación no profesional como clientes singulares de la entidad” [y abarca no sólo a] quienes realicen determinadas operaciones con las entidades, sino [a] cualquier persona que utiliza algunos de los servicios que presta una entidad financiera” (Porthé, 2008). De acuerdo a ese criterio, el carácter de cliente no está limitado por la relación contractual o precontractual, “pudiendo asignarle dicha calidad a cualquier sujeto que se acerca a la banca, haya concluido o no un negocio jurídico, en la medida en que dicho acercamiento tenga que ver con el objeto social de la entidad” (Porthé, 2008).

El usuario bancario es, por consiguiente, toda persona física o jurídica, que adquiere bienes o aprovecha servicios en forma gratuita u onerosa como destinatario final, en beneficio propio o de su grupo familiar o social. Queda equiparado al consumidor quien, sin ser parte de una relación de consumo como consecuencia o en ocasión de ella, adquiere o utiliza bienes o servicios, en forma gratuita u onerosa, como destinatario final, en beneficio propio o de su grupo familiar o social. El destinatario final es quien adquiere el bien o servicio sin intención de obtener una ganancia mediante su posterior enajenación, ni de emplearlo en un proceso de producción o comercialización de bienes o servicios destinados al mercado.

En vista de todo ello, es posible afirmar que las relaciones entre el banco y sus clientes individuos, son relaciones de consumo, en las cuales los mayores conocimientos

técnicos y profesionalidad de las entidades bancarias resultan evidentes e indiscutibles. En consecuencia, pesa sobre los bancos la obligación de brindar seguridad a los usuarios.

Completa el panorama el hecho de que, en el CCCN, los contratos electrónicos se encuentran contemplados dentro del capítulo que regula los contratos celebrados a distancia, siendo definidos por el art. 1105 como "…aquellos concluidos entre un proveedor y un consumidor con el uso exclusivo de medios de comunicación a distancia, entendiéndose por tales los que pueden ser utilizados sin la presencia física simultánea de las partes contratantes. En especial, se consideran los medios postales, electrónicos, telecomunicaciones, así como servicios de radio, televisión o prensa." En tanto, de acuerdo al art. 1106 CC: "…Siempre que en este Código o en leyes especiales se exija que el contrato conste por escrito, este requisito se debe entender satisfecho si el contrato con el consumidor o usuario contiene un soporte electrónico u otra tecnología similar…"

Operatoria bancaria y Tutela del Consumidor

Es innegable que la operatoria bancaria es una de las actividades más utilizadas en la sociedad por gran parte de la población y al mismo tiempo, es de las más complejas. Estas características, por sí solas, justifican que el Estado intervenga para regular la actividad de las entidades del sector bancario, limitando la autonomía de la voluntad de las partes al momento de contratar. Además, a todo ello se suma la especial condición de vulnerabilidad de los consumidores, que se ha calificado de "estructural", en razón de su menor poder y capacidad de negociación frente a los proveedores.

En lo que respecta a los clientes bancarios entendidos como consumidores, se dice que:

> […] el cliente-consumidor se halla en una situación de extrema vulnerabilidad, dada la complejidad y especificidad de las operatorias involucradas, y, ante todo,

> elige a la entidad bancaria en virtud de un vínculo de confianza que es constantemente avasallado por las prácticas financieras (Ritto, 2016, p. 175).

Por lo general, el consumidor bancario debe suscribir contratos ya predeterminados por las entidades, y no tiene opción: debe aceptar las condiciones de tales instrumentos o no contratar el servicio ofrecido. Por todo esto, parece plenamente justificada la necesidad de intervención del Estado en el ámbito bancario, orientada a equilibrar las fuerzas entre estos contratantes. Esto se lleva a cada mediante diversas fuentes: la ley general, el CCyC y diversas leyes especiales.

En tal sentido, debe recordarse que los usuarios bancarios, al estar comprendidos dentro de la categoría de consumidores, disponen de la tutela protectora consagrada en el plexo normativo vigente, integrado por el art 42 CN, el sistema tuitivo de la LDC, los arts. 092, 1389 y cc del CC en materia de contratos bancarios, las regulaciones administrativas aplicables a la seguridad de los clientes bancario y todas las normas nacionales e internacionales suscriptas por el Estado argentino. En consecuencia, los usuarios de servicios financieros tienen derecho en toda relación de consumo a “la protección de su seguridad e intereses económicos” según surge de la sección 2.1 inc. 1°, CO del BCRA, deber que será examinado en detalle en el siguiente apartado.

Asimismo, el art. 3 LDC, además de establecer que la "relación de consumo es el vínculo jurídico entre el proveedor y el consumidor o usuario", dispone que "En caso de duda sobre la interpretación de los principios que establece esta ley prevalecerá la más favorable al consumidor". Esta tutela se fundamenta en reconocer que los consumidores se encuentran, en las relaciones de mercado, en una situación de debilidad y vulnerabilidad estructural, genética y funcional frente a los proveedores. (Lovece, 2016).

Se ha señalado, por otra parte, que en el art. 1094 CCCN se consagra un principio interpretativo de alcance general, que junto a la norma especial y las directivas

constitucionales del art. 42 CN, consolidan a la "protección del consumidor" como principio directriz caracterizado por entender al ordenamiento jurídico de manera diferente y expansiva (Hernández, 2016, como se cita en Lovece, 2016).

En virtud de lo explicado, es posible afirmar que toda la normativa protectoria consumeril es aplicable a los contratos bancarios (entendidos en sentido amplio, como hemos visto) de modo que cualquier-usuario que sea parte de un contrato bancario puede ampararse en las previsiones de la LDC, en las regulaciones administrativas del BCRA (a través de las comunicaciones ya examinadas), en las previsiones de la LEF y lo previsto en otras leyes especiales al respecto.

Obligación de Seguridad e Hipervulnerabilidad de Consumidores en Plataformas Electrónicas

En el ordenamiento argentino, la obligación de seguridad es definida como

> […] aquella en virtud de la cual una de las partes del contrato se compromete a devolver al otro contratante, ya sea en su persona o en sus bienes, sanos y salvos a la expiración del contrato, pudiendo ser asumida tal obligación en forma expresa por las partes, ser impuesta por la ley, o bien surgir tácitamente del contenido del contrato a través de su integración sobre la base del principio de buena fe". (Barbier, 2002, p. 42).

Se ha señalado que los bancos, como intermediarios financieros, ejercen una actividad privada revestida de un intenso interés público y una función social trascendente que requiere desempeñar con profesionalidad, idoneidad y experiencia la gestión y administración de los servicios bancarios. Los bancos deben observar reglas elementales de prudencia y buena organización para precaver de todo perjuicio a sus clientes (Barreira Delfino, 2006).

En tal sentido, una de las obligaciones más relevantes de los bancos en la relación con sus clientes consiste en brindarles seguridad en los servicios que les ofrecen, lo que comprende tanto las operaciones que se desarrollan personalmente cuanto las que se realizan de manera electrónica o digital, en tanto inciden de manera directa sobre el patrimonio de los usuarios.

La obligación de seguridad es un deber secundario y accesorio que asumen expresa o implícitamente las partes en algunos contratos consistente en preservar a las personas y bienes de sus contratantes respecto de los daños que puedan ocasionarse durante su ejecución. Se sustenta en el principio de buena fe (art. 1198 CC) y, en el ámbito consumeril, en el orden público protectorio imperante en esa materia. Su utilidad práctica depende, en buena parte, de que se afecten intereses distintos al de la prestación principal. Se refiere estrictamente a los posibles daños que recaigan sobre la persona o los bienes de los contratantes con motivo de la ejecución contractual y constituye una obligación distinta de las que esencialmente impone el contrato a las partes (Pizarro, 2007, pp. 257-258)

La obligación de seguridad se desprende directamente del art. 42 CN que establece, entre los derechos básicos de los consumidores, “la protección de su seguridad e intereses económicos”. Por su parte, el art. 5 LCD impone 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. El objetivo de la figura es abarcar cualquier forma de daño que pueda afectar a la persona o a los bienes del consumidor en el contexto de una relación de consumo, garantizando la integridad de la persona y de los bienes patrimoniales y no patrimoniales involucrados en el desarrollo de dicha relación.

La CSJN dejó sentado, en "Ledesma" (331:819), la obligación de los proveedores de actividades relacionadas con la vida o salud de las personas de mantener la seguridad como valor esencial. En "Uriarte" (333:203), amplió este deber, exigiendo medidas para cumplir

leyes que protejan a posibles víctimas, evitando que los eventuales resarcimientos se vuelvan ilusorios. De acuerdo a esta interpretación pretoriana del deber de seguridad contenido en el art. 42 CN, se requiere que el proveedor adopta medidas preventivas razonables para evitar daños a los consumidores. El art. 1710, inca. b) y c) del CCC también destaca la protección de los derechos del consumidor, imponiendo al proveedor la obligación de invertir en seguridad para prevenir daños y tomar medidas preventivas frente a los productos defectuosos que ofrezca en el mercado. Asimismo, en "Mosca" (330:563) la Corte ha precisado que el deber de indemnidad abarca toda la relación de consumo, incluyendo hechos jurídicos, actos unilaterales o actos bilaterales[3].

En el contexto actual, caracterizado por la proliferación de tecnologías emergentes y formas electrónicas, digitales e informáticas de celebración de contratos, las entidades financieras se encuentran compelidas a robustecer la dimensión preventiva inherente al marco protector del consumidor. Este mandato exige la implementación de medidas concretas y eficaces en relación con los servicios digitales proporcionados a sus usuarios. La responsabilidad de asegurar la seguridad se torna aún más preeminente, considerando la integración de tecnología avanzada y el evidente aumento de su empleo, particularmente a raíz de la coyuntura experimentada durante la pandemia, lo cual ha incrementado las vulnerabilidades de los usuarios. Se ha dicho al respecto que, en el entorno digital, la obligación de seguridad a cargo del proveedor tiene carácter objetivo, en virtud de que las plataformas digitales constituyen una cosa riesgosa de acuerdo a lo establecido en el art. 1757 CCCN (Arias y Müller, 2021).

Si se tiene en cuenta que ese entorno fue organizado e impuesto por los proveedores bancarios de manera unilateral a los consumidores, conforme lo normado en los arts. 5° y 6°

[3] CSJN en "Mosca, Hugo Arnaldo c/Provincia de Buenos Aires (Policía Bonaerense) y otros s/daños y perjuicios" - Fallos: 330:563

de la ley 24.240, los riesgos derivados del mismo deben ser prevenidos por aquellos, debiendo garantizar a los consumidores igual seguridad que la exigida cuando la operación se realiza de manera presencial. Con relación a esto, se dice 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 (Carril, 2022, p. 55)

En el contexto del ámbito del derecho del consumidor, el deber de seguridad es concebida mayoritariamente como una obligación de resultado. Dicho deber se erige sobre el fundamento de asegurar la salvaguardia completa de los intereses que podrían verse perjudicados a lo largo de las fases precontractual, contractual y poscontractual. Esta obligación mantiene su vigencia incluso en el ámbito extraccontractual de la relación de consumo, especialmente en situaciones en las que personas que no son parte del contrato utilizan los servicios o se encuentran expuestas al marco de la relación consumeril con entidades bancarias. (Morea, 2022).

Los proveedores que brindan servicios o productos por vía digital están sujetos a la obligación de responder de manera objetiva, conforme al artículo 40 de la Ley 24.240 de Defensa del Consumidor, por los perjuicios derivados de ciberdelitos o delitos informáticos si sus medidas de seguridad resultaron insuficientes. Además, deben cumplir con el deber de información establecido en el artículo 4 de la misma ley, proporcionando información clara sobre los riesgos asociados a operaciones en línea y brindando recomendaciones para su uso seguro. En relación al trato a los consumidores, el artículo 8 bis de la ley impone a los proveedores digitales la obligación de ofrecer un trato justo a quienes son víctimas de

ciberdelitos, incluyendo situaciones como la sustracción de fondos bancarios o la imposición de préstamos no solicitados. La falta de respuesta adecuada de las entidades financieras puede aumentar la vulnerabilidad de los consumidores afectados y determinadas condiciones de los consumidores pueden conducir a una "hipervulnerabilidad" (COFEDEC, 2022).

En ese sentido, se considera que la vulnerabilidad tecnológica de algunos consumidores que carecen de conocimientos informáticos requiere una protección efectiva del Estado, a fin de contrarrestar la desigualdad estructural en el mercado digital. En consecuencia, se erige un marco legal que impone responsabilidades específicas a los proveedores digitales en resguardo de los derechos e intereses de los consumidores afectados por ciberdelitos en este entorno (COFEDEC, 2022).

Con relación a la expuesto, la Resolución Nº 139/2020 del Ministerio de Desarrollo Productivo, Secretaría de Comercio Interior de la Nación, haciendo referencia a "la extrema necesidad de acentuar la prevención del ciberdelito y proteger a usuarios y consumidores que por diferentes motivos se encuentra en situación de mayor vulnerabilidad o con una vulnerabilidad agravada" estableció que:

> a los fines de lo previsto en el Art. 1º de la Ley 24.440 se consideran consumidores hipervulnerables a aquellas personas que sean personas humanas y que se encuentren en otras situaciones de vulnerabilidad en razón de su edad, género, estado físico o mental, o por circunstancias sociales, económicas, étnicas y/o culturales que provoquen especiales dificultades para ejercer con plenitud sus derechos como consumidores‖.

Además, la mencionada Resolución describe en su art. 2 una serie de factores que se constituyen en causas de vulnerabilidad agravada para el consumidor, entre los que menciona ser personas mayores de 70 años, presentar alguna discapacidad, pertenecer a pueblos

originarios, ser jubilado/pensionado/trabajador en relación de dependencia con un salario menor a dos Salarios Mínimos Vitales y Móviles y ser monotributista social, entre otros.

Capítulo IV

Responsabilidad Bancaria

Para determinar la responsabilidad de los proveedores bancarios que ofrecen o comercializan sus servicios mediante plataformas digitales o la red Internet por los fraudes cometidos contra los usuarios, corresponde desarrollar un diálogo coherente y armónico entre las distintas fuentes del ordenamiento jurídico a partir del paradigma protectorio del consumidor

La teoría del riesgo, en sus diversas formulaciones, postula que un sujeto es responsable por los riesgos generados por su acción, aún si ejerce la diligencia debida para prevenir daños. Variantes como la teoría del riesgo beneficio han surgido como base de explicación para situaciones de responsabilidad civil que no encajaban en la doctrina tradicional. Según esta teoría, quien obtiene beneficios de una actividad o cosa debe asumir los riesgos inherentes, ya que quien se beneficia debe afrontar los peligros y los daños relacionados con dicha actividad o bien. Se acepta que esta teoría se incluya en marcos legales, no como norma general, sino para justificar casos excepcionales expresamente previstos por la ley.

Los arts. 1066 y 1067 CC establecen los elementos que configuran la ilicitud civil: violación del ordenamiento jurídico (elemento objetivo), acto voluntario imputable al agente (elemento subjetivo) y la existencia del daño (elemento externo). Se subraya que la prohibición debe derivar del conjunto del sistema jurídico, no de una norma aislada.

Así, la responsabilidad puede ser subjetiva, basada en la culpa (dolo o culpa en sentido amplio), donde el sujeto debe cumplir todos los requisitos doctrinales y legales. Por otro lado, la responsabilidad objetiva prescinde de la culpabilidad y hasta de la voluntariedad.

En esta última, es esencial la existencia del resultado dañoso y un vínculo causal material con el sujeto responsable. Por ejemplo, si un individuo inimputable causa daño, debe responder por equidad (artículo 907, nuevo).

Según Gallaso (2010), actualmente la tendencia de la responsabilidad objetiva ocupa un lugar más importante que la culpabilidad porque los supuestos más relevantes de responsabilidad civil recaen bajo su órbita, como la responsabilidad del principal por el hecho del dependiente, daños causados por el riesgo o vicio de la cosa o por actividades riesgosas, responsabilidad de las personas jurídicas, incumplimiento de obligaciones de resultado, entre otras. En estos casos, el banco tiene una obligación de resultado para con el cliente, que es la de resguardar el dinero depositado a su confianza y garantizar el acceso a la cuenta bancaria solamente al cliente o a las personas que él designe y cuando él lo desee. Por ello su falta de diligencia conduce al incumplimiento de la obligación, resultando aplicable la teoría del riesgo, según la cual "quien realiza actividades que por su naturaleza o modo de empleo generan riesgos potenciales a terceros, debe responder por los daños que ellas originan". La autora mencionada cita a Vallespinos y Pizarro quienes reafirman su apoyo a esta teoría, y argumentan que quienes introduzcan al medio social un factor generador de riesgos deben responder objetivamente, se beneficien o no con el mismo, a que la responsabilidad objetiva deriva de la creación del riesgo y no del posible beneficio que de él deriva.

Conviene repasar brevemente, en este punto que la buena fe en sentido amplio equivale al género y es comprensiva de dos especies: la buena fe subjetiva o creencia y la buena fe objetiva o lealtad/probidad. La primera es la creencia o confianza de que se está actuando conforme a derecho y por lo tanto existe una total ignorancia de la antijuricidad del comportamiento, es decir, como apunta Mosset Iturraspe (1997) que la persona ignora que su proceder está generando un perjuicio a otro; y esta situación acontece precisamente porque la persona tiene la creencia de que posee legítimamente un derecho.

A su vez la buena fe objetiva o lealtad/probidad hace referencia a la conducta o proceder del sujeto que debe estar enmarcada dentro de los parámetros de lealtad y honestidad, y observarse durante todo el proceso negocial. Es decir que se trata de un modelo de conducta a seguir. En síntesis, se puede inferir que en lineamientos generales coinciden en que se trata de una responsabilidad distinta a la que recae sobre el empresario común, una responsabilidad que se presenta como una responsabilidad agravada.

Se ha destacado, en tal sentido, que la actividad que llevan adelante los bancos y de las entidades financieras están subordinadas de manera cada vez más directa al factor de atribución objetivo, lo que tiene su correlato en la tarea de superintendencia que desarrolla el BCRA cuando revisa ciertas conductas de las entidades (Liendo, 2016).

La responsabilidad agravada tiene su sentido de ser en que el grado de desarrollo y el crecimiento mismo del negocio bancario está fuertemente relacionado con la confianza de los clientes. exige un alto grado de profesionalidad dado que al captar y manejar el ahorro público deben maximizar los cuidados a fin de evitar su pérdida o disminución; tampoco puede soslayarse la enorme repercusión que el manejo y comportamiento negocial (sea positivo o negativo) tiene en la dinámica económica y política de un país (Arduino, 2013).

La confianza que el usuario deposita en la entidad bancaria dependerá del cumplimiento de las “buenas prácticas bancarias” antes mencionadas y de la “buena gestión que hagan sus directivos, ya que se trata de una actividad de calificada” lo que determina el agravamiento de su responsabilidad, carácter que ha sido ampliamente reconocido tanto doctrinaria como jurisprudencialmente. Se habla de profesiones calificadas.

Al tratarse de una problemática relativamente novedosa se denotó la ausencia de una normativa especial para regular la responsabilidad de las entidades bancarias, lo que conllevó que para resolver los conflictos se recurriera a la aplicación del derecho común .Es necesario en tal sentido tener especial tratamiento, de las partes vinculadas por esa relación negocial, la

que se manifiesta una diferencia importante frente a un determinado conflicto en cuanto a medios y posibilidades a fin de determinar en la forma más equitativa las responsabilidades y darles el encuadre jurídico correcto.

Ante tal situación en un principio, los diferentes conflictos planteados con los bancos, su responsabilidad —sea contractual o extracontractual— se recurría a la aplicación de los arts. 506, 511, 512, 519, 1067, 1068, 1083, 1109, 1113 y concordantes. La falta de una norma específica en el Código de Vélez que regule el conflicto en estudio se debió a que se consideraba que no era propio de un cuerpo normativo incorporar nociones de tipo exhortativo por ser éstas amplias e imprecisas (Mosset Iturraspe, 1997, 261).

No obstante, en la Sección Segunda del Libro Segundo, en el Título I, "De los Hechos" establecía una relación de mayor responsabilidad en la medida que el obrar exigiera un grado superior de cuidado o competencia. Así, el art. 902 disponía: "Cuanto mayor sea el deber de obrar con prudencia y pleno conocimiento de las cosas, mayor será la obligación que resulte de las consecuencias posibles de los hechos". esta normativa ya nos proporciona un parámetro a la hora de determinar el grado de responsabilidad de las partes.

Pero recién con la reforma introducida por la Ley 17.711 que se incorporó el principio de la buena fe al tema de los contratos, con el texto al artículo 1198

Esto va reforzando la idea que el carácter profesional resulta un factor de suma importancia para ponderar el comportamiento de la institución bancaria y determinar el grado de su responsabilidad. Concretamente con la sanción de la Ley 26.994 el 1º de octubre de 2014, se introdujeron algunos cambios de suma importancia sobre la responsabilidad de las instituciones bancarias.

Así el nuevo código en el Capítulo 3 del Título Preliminar, al referirse al "Ejercicio de los Derechos", incorpora como principio general a la "buena fe" (art.9); y precisamente el lugar de su ubicación dentro del código implica otorgarle un lugar de preeminencia en todo el

derecho privado. Además, junto con los artículos siguientes referidos al “abuso del derecho” (art.10) y al “abuso de posición dominante” (art.11) conforman, más allá del mandato normativo que contienen, una pauta de interpretación hábil a tener en cuenta por los jueces para orientar sus decisiones.

Estos aspectos sumamente importantes concretos y novedosos sobre la buena fe, abuso del derecho y abuso de posición dominante — en el Título Preliminar reafirma la voluntad legislativa de elevarlos al rango de reglas generales del derecho positivo argentino y como guía interpretativa para valorar la conducta desplegada por las personas, sean humanas o jurídicas .A ´partir de esas directivas, la conducta de la empresa bancaria deberá ceñirse a tales reglas, so pena de incurrir en responsabilidad.

En la nueva codificación se contempla expresamente el principio alterum non laedere (no dañar a otro) al cual la Corte Suprema había reconocido carácter constitucional. Así el Art. 1710 el “deber de prevención del daño” que es la consagración normativa establece que: toda persona tiene el deber, en cuanto de ella dependa, de:

a) Evitar causar un daño no justificado;

b) Adoptar, de buena fe y conforme a las circunstancias, las medidas razonables para evitar que se produzca un daño, o disminuir su magnitud; si tales medidas evitan o disminuyen la magnitud de un daño del cual un tercero sería responsable, tiene derecho a que éste le reembolse el valor de los gastos en que incurrió, conforme a las reglas del enriquecimiento sin causa;

c) no agravar el daño, si ya se produjo.

Esta obligación comprende a “toda persona” sin hacer ningún tipo de distinción entre persona humana y persona jurídica, por consiguiente, es perfectamente aplicable a las instituciones bancarias. Asimismo, el artículo fija dos parámetros — buena fe y

razonabilidad— para analizar las circunstancias de cada caso en particular. Es indudable se encuentran mayormente exigidos a quienes tengan una profesión calificada como los bancos.

Por su parte el art.1723 CCC, dispone que en el caso de las obligaciones de resultado la responsabilidad que derive de ellas será "objetiva", siendo evidente que hay un agravamiento de la responsabilidad para los bancos; Es que la calificación de "objetiva " de la responsabilidad derivada de las obligaciones de resultado puso en manto de claridad sobre una cuestión instalada desde hace muchos años, ya que ahora queda claro que en este tipo de obligaciones para eximirse no se podrá alegar sobre las cualidades del accionar de la empresa financiera, ya que esta tiene obligación de resultado y no puede alegar responsabilidad subjetiva de sus clientes.

El art. 1724, también introduce cambios importantes en lo atinente a la responsabilidad, en la medida que no se requiere que la acción se ejecute para causar un daño, ya que conforme el texto legal en vigencia si el agente "desdeña el perjuicio que puede ocasionar" (Picasso y Saénz, 2015) resultará responsable.

Por su parte el art. 1725 se refiere a la "valoración de la conducta" al contemplar en su primera parte que se trata de una proporción directa, a mayor conocimiento o profesionalidad mayores serán las exigencias del cumplimiento y mayor responsabilidad. Se puede concluir que este proceso de actualización que fue se fue aplicando en nuestra legislación civil, resalto y puso de manifiesto las nociones sobre responsabilidad aplicables a las negociaciones bancarias, y con ello proporciono de mayores herramientas legales al juzgador a la hora de resolver los conflictos planteados en el tema de estudio.

La ley 24.240, de protección al consumidor, en su art. 5, se refiere al deber de seguridad, de los usuarios, la interpretación debe ser amplia abarcando todas las situaciones de las cuales durante el desarrollo del contrato se pueda derivar algún daño para los usuarios. Ante este encuadramiento, los proveedores bancarios y financieros asumen la responsabilidad

objetiva que trae el art. 40 de la Ley 24.240, y solo podrán eximirse de su responsabilidad demostrando los eximentes previstos para este tipo de responsabilidad, que es que el daño fue causado por una causa ajena, un tercero por el que no debe responder, caso fortuito o fuerza mayor, o culpa de la víctima

Con relación a ello, se expresa:

> Ahora bien, que el cliente bancario fuera considerado un consumidor y la relación en cuanto a las prestaciones que contrata con el Banco y servicios que este le presta estén regidas por la LDC, con anterioridad a la sanción del Código Civil y Comercial, era aceptado mayoritariamente por la doctrina y por no poca jurisprudencia. Sin embargo, las entidades bancarias oponían como defensa que la relación debía juzgarse por el Código Civil (CC), siendo errónea la aplicación de la ley 24.240.

Al respecto, según Muñoz Barda (2014, como se cita en Saires y Héctor, 2022), a pesar de las discusiones previas, se fue consolidando un consenso sobre la aplicabilidad de la Ley de Defensa del Consumidor (LDC) a las relaciones entre entidades bancarias y clientes. Este punto de vista el sistema civilista plasmado en art. 1384 CC, al establecer ─como se analizó en el capítulo anterior─ que las disposiciones sobre contratos de consumo son extensibles a los contratos bancarios celebrados después de su promulgación.

Al examinar la responsabilidad de los bancos, Abad (2016) toma como punto de partida las disposiciones del BCRA y examina un conjunto de fallos relevantes de la jurisprudencia nacional, considerando palpable la responsabilidad bancaria ante las estafas electrónicas en base a su deber de informar y proteger a los consumidores, a quienes se impone el uso de un sistema de homebanking aparentemente confiable, que debe brindarles la misma seguridad que la exigida cuando la operación se realiza de forma personal. Asimismo, menciona algunas medidas que permitirían prevenir la comisión de operaciones fraudulentas,

previstas en un conjunto de disposiciones del BCRA a la que se ha hecho referencia en el primer capítulo de este trabajo.

La Culpa o el Hecho del Consumidor como Eximentes de Responsabilidad

De conformidad con los cánones generales establecidos en el sistema de responsabilidad civil por daños del Código Civil y Comercial de la Nación, la doctrina de la culpa de la víctima, la intervención de terceros por la cual no se debe responder y la ocurrencia de caso fortuito o fuerza mayor, despliegan su función eximente en el contexto de la responsabilidad objetiva, al operar como elementos causales que interrumpen la cadena causal, y por consiguiente exoneran al deudor de responsabilidad .

Esta regla de evaluación restrictiva de la culpa del consumidor conlleva que no cualquier acto imputable a este último tenga el poder de interrumpir la cadena causal, sino que es requisito que tal acto pueda ser equiparado con la ocurrencia de un evento fortuito ajeno. En otro sentido, esta regla en cuestión es un distintivo característico del microsistema protector de los consumidores, lo cual lo aparta del régimen general de responsabilidad y desempeña un papel esencial para la comprensión de su funcionamiento y su aplicación en la jurisprudencia (Sozzo, pp. 149-150).

Desde esta perspectiva, el acto del consumidor debe presentar características de imprevisibilidad, inevitabilidad y ajenidad respecto al proveedor. Con respecto a este último elemento, se reputará que el acto será ajeno no solamente porque tenga lugar fuera del ámbito de actuación del presunto responsable, por el cual debe asumir responsabilidad (art. 1733 inc. d CCC) sino también porque debe ser ajeno al riesgo inherente a la cosa o actividad desplegada (art. 1733 inc. E del CCC). Estos dos aspectos del requisito de ajenidad adquieren un significado particular desde la perspectiva del Derecho del Consumidor: El primero se torna más riguroso al considerar que el acto no es ajeno si puede ser imputado a un integrante de la cadena de producción o comercialización del producto, b) el segundo aspecto se

relaciona con la noción de profesionalismo del proveedor y amplía el estándar de previsibilidad que el proveedor debe mantener en relación con el riesgo inherente a su actividad.

De este modo, se advierte que el alcance de la causal eximente se ve notoriamente restringido, y solo en casos excepcionales el consumidor será privado de la posibilidad de obtener reparación. Esta circunstancia se materializará únicamente cuando su conducta denote un desprecio por las precauciones más elementales que pudieran estar a su disposición, o cuando su actuación revele una imprudencia activa, es decir, un esfuerzo directamente dirigido a desafiar las normas de seguridad (Stiglitz, G. (2015, pp. 359-362).

Este aspecto ilustra de manera evidente la eficacia protectora del derecho del consumidor al impedir la exoneración del deudor-proveedor y al promover la indemnización de los daños sufridos por la parte vulnerable de la relación contractual. La construcción de este enfoque jurídico encuentra fundamentación en los principios generales que rigen el derecho del consumidor, en particular el principio de protección (art. 42 CN, art. 1094 CCC y art. 1 LCD) y en la regla hermenéutica que demanda la interpretación favorable al consumidor (art. 1094 in fine CCC y art. 1 LCD).

Jurisprudencia Relevante

Existen diversos precedentes en la jurisprudencia argentina referidos a la asignación de responsabilidad de entidades bancarias como resultado de fraudes electrónicos contra sus clientes. A continuación, se mencionan algunos fallos relevantes

El leading case en la materia es el caso “Bieniauskas, Carlos c/ Banco Ciudad”[4] en el cual los magistrados de la Sala D de la Cámara Nacional de Apelaciones en lo Comercial, Gerardo G. Vassallo - Juan J. Dieuzeide sentaron un precedente decisivo al confirmar la

[4] Cámara Nacional de Apelaciones en lo Comercial, sala D en autos: Bieniauskas, Carlos c. Banco de la Ciudad de Buenos Aires, 15/05/2008, La Ley: AR/JUR/3631/2008

decisión de primera instancia que había hecho lugar a una acción de daños y perjuicios contra el Banco Ciudad de Buenos Aires presentada por un usuario de la tarjeta de débito otorgada por esa entidad.

Ese cliente había suministrado su clave de extracción para cajeros automáticos a personas que ─fingiendo ser empleados de la entidad bancaria─ se comunicaron con él telefónicamente y se la pidieron, argumentando que necesitaban conocerla para investigar supuestos casos de uso de tarjetas apócrifas. Posteriormente, usando tarjetas "mellizas", lograron extraer fondos de la cuenta del titular de la tarjeta. Ante esa situación, la víctima reclamó al banco por el perjuicio ocasionado sin obtener ninguna solución, por lo que decidió demandar a la entidad

El fallo de primera instancia condenó a la demandada por considerarla responsable de los daños sufridos por el actor. La demandada presentó una apelación contra la sentencia, por lo que debió intervenir la Cámara que decidió confirmar el fallo condenatorio, entendiendo que la entidad tiene responsabilidad por los daños causados por la extracción fraudulenta de los fondos que el actor tenía depositados en su caja de ahorros

El texto resalta que la negligencia de la víctima al proporcionar su clave a terceros no exime de responsabilidad al banco, ya que la existencia de la posibilidad técnica de duplicación de tarjetas pone en evidencia la vulnerabilidad del sistema informático empleado para los servicios remotos, considerándose como una cosa riesgosa. Además, esta circunstancia demuestra que la conducta del cliente resulta irrelevante, dado que los conocimientos técnicos de los perpetradores son esenciales para llevar a cabo la actividad delictiva.

Incluso en presencia de una imprudencia especialmente grave por parte del consumidor, se argumenta que el banco, en su calidad de experto en la materia, tenía la obligación de prever y prevenir este tipo de situaciones mediante medidas adecuadas. Se

subraya que, en la relación entre banco y cliente, se aplica una interpretación rigurosa de la conducta del banco debido a su experiencia y posición ventajosa en la industria bancaria. Por lo tanto, se concluye que las entidades bancarias, al contar con la información y habilidades técnicas, son responsables de proporcionar seguridad y, si es necesario, brindar la evidencia necesaria para el entendimiento completo del caso ante el juez.

Este fallo ejemplifica cómo en situaciones particulares, incluso ante una negligencia grave por parte del consumidor, el banco puede ser considerado responsable por el daño sufrido por este último.

En 2019, la Corte Suprema de Justicia de Santa Fe confirmó el fallo de la Cámara de Apelación en lo Civil y Comercial de Rosario-Sala Cuarta que había condenado al Banco Macro a resarcir económicamente a la actora, cliente de la entidad bancaria que había sido víctima de una estafa electrónica y decidió accionar por daños y perjuicios. El argumento central empleado por el Tribunal para fundar su decisión fue el siguiente: “Que tanto la obligación tácita de seguridad derivada del principio de la buena fe imperante en materia contractual, como el deber de la entidades bancarias-exigible a partir de las reglamentaciones del Banco Central- de garantizar mediante mecanismos de seguridad informática la genuinidad de las operaciones realizadas en forma no personal (electrónica, telefónica, vía “internet”, etc.) constituyen obligaciones de resultado, configurando su incumplimiento un supuesto de responsabilidad objetiva que, aún si se admitiera hipotéticamente el escenario propuesto por la demandada y acogido en la instancia anterior, en el sentido de que la actora habría recibido la tarjeta de coordenadas y culposamente habría revelado las claves a terceros, ello no permitiría concluir en la ruptura del nexo causal, al no revestir esa eventual culpa de la víctima los caracteres de imprevisibilidad o inevitabilidad, aun cuando la culpa de la entidad bancaria no tendría mayor relevancia por tratarse de un supuesto de responsabilidad

objetiva, igualmente aparecía configurada, al no haber actuado aquélla con la diligencia que cabría esperarse de un comerciante especializado con alto grado de profesionalidad."[5]

Sin embargo, existen antecedentes que, al resolver la responsabilidad de los bancos en casos similares, decidieron en sentido contrario al expuesto.

Por ejemplo, en "Cipriano, Ricardo José y otro c/ Banco Credicoop Coop. Ltdo. s/ Ordinario" la Sala F de la Cámara Nacional de Apelaciones en lo Comercial de la Ciudad Autónoma de Buenos Aires, el 28 de diciembre de 2020 confirmar la sentencia dictada en primera instancia, absolviendo de responsabilidad a la entidad bancaria demandada por los daños y perjuicios peticionados

El actor era un cliente de la entidad, que fundamentó la demanda en una alegada falta de medidas de seguridad que protegieran de manera adecuada el sistema implementado de homebanking implementado en la plataforma informática ofrecida por la entidad financiera, y la presunta falta de información suficiente acerca de los servicios prestados por la misma.

El fundamento central del decisorio era que el deber de seguridad a cargo del banco para proteger a sus clientes no puede controvertirse, pero que no consiste en una obligación de resultado, como sostenía la demanda, sino una obligación de medios, que impone la adopción de medidas preventivas, pero no se extiende más allá de las circunstancias riesgosas previsibles.

En el expediente, la entidad demandada ofreció como prueba a su favor distintas pericias informáticas que acreditaron la existencia de suficientes medidas de seguridad para prevenir eventuales actos fraudulentos cuando se cometió el delito, alegando que no se presentó ninguna situación que permitiera advertir ni sospechar la posible comisión de un fraude. La Cámara aceptó dicho argumento y entendió acreditado que el Banco había

[5] Corte Sup Just de Santa Fe en autos "Red del Interior S.R.L. c/ Banco Macro S.A. s/DAÑOS Y PERJUICIOS – (Expte. 317/16-CUIJ 21-01322251-4)", Reg: A y S t 288 p 334/340, 12/03/2019.

cumplido adecuadamente el deber de seguridad en la plataforma de banca electrónica puesta disposición de sus clientes. En tal sentido, consideró que ─mediante la pericia realizada por un ingeniero en sistemas─ se probó la implementación de sistema de doble validación con clave con función hash sha-1.

Al resolver, la Cámara argumentó que "la relación jurídica sometida a juzgamiento desde el deber de seguridad, sea que se lo considere incorporado al vínculo por fuente constitucional (conf. arg. art. 42 de la CN) o legal (art. 5 LDC), evidente resulta que pesaba sobre el banco la obligación de adoptar aquellas medidas de prevención que fueran adecuadas a los concretos riesgos existentes en orden a la actividad profesional realizada" y que "el deber de seguridad no podrá considerarse como una obligación de resultado que conlleve un factor de atribución objetivo, como propenden los accionantes y la Representante del Ministerio Público Fiscal ante esta Cámara", remarcando que "no es posible afirmar la existencia de una garantía de resultado, de manera que el usuario no sufra daño alguno".

Esta postura reconoce de manera más amplia la limitación de responsabilidad de las entidades financieras que el criterio expuesto por la jurisprudencia mayoritaria, ya que reconoce que, sin perjuicio de las medidas de seguridad que las entidades financieras apliquen, pueden producirse ilícitos que excedan la capacidad de las referidas entidades para evitarlos. Esto pone en cabeza de los clientes un cierto grado de responsabilidad por el manejo de las transacciones electrónicas realizadas. El fallo consideró que "(..) Credicoop adoptó la conducta esperable conforme su especialización. Ello en tanto no fue advertida por el experto ninguna circunstancia anómala en el desarrollo de dichas transacciones".

Por otra parte, se consideró que la demandada también había dado cumplimiento al deber de información, entendiendo que la entidad había acreditado mediante la documentación acompañada oportunamente al proceso que brindó a los usuarios suficiente información a fines de evitar cualquier tipo de fraude o el robo de información. Entendió

acreditada la circunstancia de que en el sitio web del Banco se advertía de manera clara y precisa a los usuarios acerca de tener cuidado de no entregar sus datos bancarios a terceros que se los soliciten, subrayando que “la demandada brindó la información necesaria para que los accionantes pudieran llevar a cabo todas las operaciones necesarias a través de la Banca Internet sin ser sujetos de defraudaciones o fraudes”, responsabilizando a los propios usuarios por el uso inadecuado del Homebanking, señalando, en tal sentido que “no tengo dudas de que éstos no ejecutaron adecuadamente las medidas de seguridad informadas por el banco accionado, lo que propició ser sujetos de algún tipo de defraudación”.

Se puso de manifiesto, por otra parte, un criterio que niega considerar riesgoso al sistema informático, entendiendo, en cambio que el mismo es una cosa inerte. Por consiguiente, no puede calificarse a dicho sistema como actividad riesgosa y no es correcto que se encuadra dentro de los presupuestos del artículo 1757 del Código Civil y Comercial de la Nación.

Un criterio similar utilizó la Sala Primera en lo Civil y Comercial de la Cámara de Apelaciones de Gualeguaychú en "G., B. I. c/ Nuevo Banco de Entre Ríos S.A. s/ sumarísimo", al revocar una sentencia que condenó al Nuevo Banco de Entre Ríos por una demanda de una clienta afectada por una estafa telefónica, con fecha 22 de mayo de 2017. La demandante fue engañada por un tercero que obtuvo sus claves bajo la premisa de otorgarle un premio, lo que permitió al delincuente operar en su cuenta bancaria y solicitar un préstamo. La sentencia de primera instancia atribuyó responsabilidad concurrente a ambas partes, condenando al banco por el 50% del reclamo. Sin embargo, en apelación, la Cámara revocó la sentencia al considerar que las medidas de seguridad del banco no podrían haber impedido la conducta negligente de la demandante al compartir sus claves bajo engaño.

La Cámara analizó las obligaciones del banco respecto a la seguridad y el deber de advertencia. Se hizo hincapié en la imposibilidad de prever todas las situaciones posibles y se

destacó la necesidad de educar al consumidor en la protección de sus claves. La Cámara cuestionó la falta de especificidad en las acusaciones sobre las omisiones del banco y subrayó que las medidas de seguridad, aunque importantes, no son suficientes si no se ejerce prudencia por parte del consumidor. Por ende, se concluyó que la responsabilidad del banco era limitada en esta situación, y se revocó la condena en su contra. La decisión se basó en el principio de que las medidas de seguridad implementadas por el banco no pueden ser responsables por las acciones negligentes de los consumidores y que la educación del cliente es fundamental para evitar situaciones como esta.

En el contexto de un caso de phishing, el Superior Tribunal de Justicia de Jujuy emitió un fallo el 22 de mayo de 2017 en "Salum, Andrés Alejandro c/ Banco Santander Río S.A.", donde confirmó la responsabilidad de la entidad bancaria y ordenó un resarcimiento civil al actor. En el marco de la "responsabilidad objetiva", el tribunal estableció que el Banco incumplió su compromiso de custodiar el dinero depositado por el actor al entregarlo a un tercero no autorizado a través de un cajero automático. Aunque se planteó la permeabilidad del sistema de seguridad del Banco, el tribunal sostuvo que, en un supuesto de responsabilidad objetiva, el Banco debía resguardar los fondos confiados en custodia sin importar la eficacia del sistema de seguridad. La obligación era de resultado, y el Banco debía responder por la indebida detracción de fondos, independientemente de las conclusiones de un perito. Se destacó que la verdadera víctima de los piratas informáticos fue la entidad bancaria, ya que burlaron sus medidas de seguridad. La decisión del tribunal a quo de no producir una prueba inconducente fue considerada razonable en el contexto del caso.

En el caso "Roda, Ramona Lujan, c/ Nuevo Banco de Santa Fe SA s/ demanda de derecho de consumo", el Juzgado de Primera Instancia en lo Civil y Comercial 1ra. Nominación de Reconquista, Provincia de Santa Fe, en su resolución del 03/03/2021, acogió la demanda de una consumidora y declaró la ineficacia por nulidad del acto jurídico

impugnado (contratación de un préstamo por medios electrónicos). El tribunal argumentó que el acto ilícito fue efectivamente dirigido contra la entidad bancaria, y que el cliente fungió como una vía empleada por el delincuente informático para llevar a cabo su acción delictiva. En este contexto, el juez fundamentó que, en concordancia con la eficacia orientada a objetivos, debe resaltarse que la equidad ha transformado su papel, evolucionando de ser un criterio interpretativo (introducido en la reforma proyectada en 1968 para abordar situaciones injustas) en una fuente autónoma de derechos dentro del nuevo Código. Bajo esta perspectiva, el juez concluyó que, por motivos de equidad, no sería apropiado que el cliente bancario afrontara las consecuencias de un acto delictivo cometido contra la entidad, ya que el banco, en calidad de proveedor de un servicio público, tiene la responsabilidad de otorgar a sus usuarios un trato digno. En este sentido, consideró que la dignidad del usuario se vería menoscabada si, al conocer los detalles del delito, el banco ignorara la situación y buscara cobrar a la cliente el capital e intereses como si nada hubiera ocurrido.

La Cámara de Apelaciones de Viedma rechazó el recurso de apelación presentado por el Banco Patagonia S.A. en contra de la sentencia de primera instancia que admitió una demanda por daños y perjuicios, declaró la invalidez de un préstamo tramitado por intermediarios mediante la plataforma de homebanking y condenó a la entidad bancaria al pago de una indemnización pecuniaria. La resolución del superior determinó que la víctima no incurrió en negligencia, sino que las debilidades identificadas en el sistema bancario, a pesar de ciertas mejoras actuales, permitieron que la demandante y numerosos individuos más fueran víctimas recurrentes de tales fraudes. Además, se añadió que la entidad financiera exhibió un control insuficiente para prevenir la consumación de la maniobra delictiva en cuestión.[6]

[6] Câm de Apel Civ, Com, Fam y Min 1°, Viedma - Expte. N° Vi-31306-C-0000 - “Bartorelli, Emma Graciela c/ Banco Patagonia S.A. s/ Daños y Perjuicios (Sumarísimo)” - 29/09/2022.

El 4 de octubre de 2021, la Sala IV de la Cámara Contencioso Administrativo Federal rechazó el recurso de apelación presentado por el Banco Santander Río S.A. contra la Disposición 452/21 del Ministerio de Desarrollo Productivo, que había impuesto a la entidad una multa de $5.000.000, fue rechazado. La imposición de la multa se fundamentó en la infracción de los arts. 4, 5, 8 bis y 19 de la Ley 24.240, debido a las siguientes razones: i) La entidad bancaria no proporcionó información precisa, comprensible y detallada sobre los riesgos asociados a su actividad comercial. ii) La falta de cumplimiento de la obligación de brindar un servicio seguro permitió que terceros llevaran a cabo estafas mediante la tecnología proporcionada por el banco, afectando a los clientes y permitiendo el acceso no autorizado a sus cuentas y transacciones. iii) Los reclamos de los afectados no fueron atendidos adecuadamente, lo que resultó en una falta de atención digna y equitativa hacia los consumidores. iv) Los términos, condiciones y modalidades del servicio no se ajustaron a lo ofrecido, publicitado o acordado[7].

También en Viedma, el 2 de noviembre de 2021, el Juzgado Civil, Comercial, Minería y Sucesiones N° 1 declaró la nulidad de un contrato de préstamo generado mediante la plataforma de homebanking del Banco Patagonia S.A. y condenó a esa entidad a resarcir y devolver los montos debitados en concepto de cuotas a una de sus usuarias. El Tribunal consideró como argumento central de su decisión, que el banco demandado debió implementar un sistema de alerta para prevenir y detectar de manera oportuna posibles conductas fraudulentas que ocurran en las transacciones realizadas a través del sistema online disponible para sus clientes[8].

[7] Câm. Cont. Adm. Fed. Sala IV - Expte. N° 19719/2021 - "Banco Santander Río S.A. c/ En-M Desarrollo Productivo (Ex 3316571/21 - Disp. 452/21) s/ Recurso Directo Ley 24.240 - Art. 45" - 04/10/2022.

[8] Juzg. Civ. Com, Min. y Suc.N° 1, Viedma. Expte. N° Vi-14379-C-0000, "Linares, Marcela Valeria C/ Banco Patagonia S.A. S/ Daños Y Perjuicios (Sumarísimo)", 02/11/2022.

Los antecedentes examinados reflejan la complejidad inherente a la resolución de controversias de esta índole, puesto que el enfoque para asignar responsabilidad demanda un análisis minucioso de los eventos, así como del papel desempeñado por las víctimas y perjudicados, en virtud de una interpretación sistémica, comprensiva y coherente del ordenamiento jurídico.

La revisión de la labor interpretativa llevada a cabo por los magistrados argentinos al dirimir casos de responsabilidad civil bancaria permite identificar la consolidación de una posición mayoritaria que aboga por la aplicación de una responsabilidad objetiva a las instituciones bancarias en situaciones de fraude electrónico dirigido a sus clientes. Esta perspectiva se fundamenta en el paradigma protector de los consumidores y halla sustento en el deber de seguridad que recae sobre los proveedores de servicios bancarios electrónicos, reforzado por los riesgos inherentes a dicha actividad y la naturaleza profesional de dichos actores. Dicha responsabilidad se erige como objetiva y se interpreta de manera restringida en lo que concierne a la eventual exoneración de responsabilidad del proveedor frente a los perjuicios infligidos a los consumidores, considerando la vulnerabilidad estructural de estos últimos y su extrema susceptibilidad al operar en entornos electrónicos.

Conclusiones

Es posible concluir, de acuerdo al marco legal vigente en materia de responsabilidad civil en el ordenamiento argentino, las instituciones bancarias tienen responsabilidad en relación con los actos ilícitos perpetrados contra sus usuarios a través de medios electrónicos. Esta obligación deriva del deber de seguridad que recae sobre las entidades bancarias; en virtud del sistema de obligaciones, se espera que estas entidades anticipen posibles fallos de seguridad que puedan afectar a quienes utilizan sus servicios, y que tomen las medidas necesarias para mitigar dichos riesgos.

La actividad bancaria es una actividad profesional con una valoración agravada por la posición que ocupa; los medios electrónicos y cibernéticos de operaciones bancarias tales como el homebanking son cosas riesgosas según el desarrollo jurisprudencial mayoritario; por otra parte, los usuarios financieros mientras se encuentren en la cartera de consumo tienen la protección de todo el sistema consumeril. Desde esta perspectiva, no corresponde limitar la responsabilidad de la entidad bancaria en casos de fraude cibernético por el solo hecho de que el proveedor haya informado el peligro a sus clientes

Al respecto, aunque existen diferentes criterios empleados por los tribunales para ponderar la responsabilidad bancaria en tales supuestos, la jurisprudencia argentina se ha inclinado mayoritariamente por considerar aplicable tal responsabilidad, teniendo en cuenta las particularidades de cada caso. Las disimiles características y modalidades de estafa cibernética observadas empíricamente imponen evaluar cada supuesto en particular a fin de poder determinar el grado de responsabilidad que puede tener la entidad bancaria involucrada, eximiéndola de responder con criterio fuertemente restrictivo.

La mayoría de los precedentes jurisprudenciales ponen en cabeza del banco el deber de seguridad, por entender que encierra una obligación de resultado y no una de medios. De esta manera, asumiendo que la entidad bancaria cuenta con superioridad técnica, económica y de conocimiento, consideran que los bancos deben adoptar una conducta de protección del usuario, en atención al carácter de vulnerabilidad estructural de los mismos en tanto consumidores. A esto se suma el criterio de contemplar la situación de hipervulnerabilidad en casos de consumidores que merecen una mayor protección, como por ejemplo ocurre con las personas mayores, clientes obligatoriamente bancarizados que muchas veces desconocen cómo operar en canales cibernéticos y suelen ser víctimas de quienes aprovechan tal condición.

Por otro lado, un sector minoritario de los tribunales sostiene que el deber de seguridad del banco se encuentra limitado en aquellas ocasiones en las que el cliente brinda voluntariamente sus claves, accionar negligente que impide asignar responsabilidad alguna a la entidad que arbitró las medidas de seguridad exigibles para prevenir el riesgo de daño a los usuarios de sus servicios.

No puede soslayarse que el crecimiento de casos de fraude electrónico en perjuicio de los consumidores bancarios representa una amenaza para la sociedad. Este fenómeno requiere de una respuesta coordinada por parte de las instituciones públicas y privadas (las propias entidades bancarias y otras empresas del sector financiero, las organizaciones de la sociedad civil).

Las entidades del sector bancario deben profundizar en la adopción de mecanismos de regulación, protección y mitigación de riesgos ante posibles ataques digitales para no dejar desamparados a usuarias y usuarios. Ello requiere de la adopción de protocolos, mayores inversiones, realizar acuerdos e implantar estándares más estrictos de ciberseguridad. Por ejemplo, actualmente se dispone de tecnologías disruptivas como el Blockchain y la Inteligencia Artificial, que pueden ser herramientas importantes para crear un entorno de mayor seguridad en favor de las operaciones de intermediarios en el ámbito de la banca comercial relacionada con la cartera de consumidores. Este tipo de tecnologías se destaca por ofrecer algunas soluciones dirigidas a mejorar la protección de datos y la eficiencia transaccional de la operatoria bancaria.

Finalmente, se concluye que el principio de seguridad debe prevalecer, tanto para los usuarios de la banca electrónica como para las propias instituciones financieras. La adopción de medidas de prevención y mitigación, la implementación de salvaguardias tecnológicas y la transparencia en las políticas de protección de datos se erigen como piedras angulares para edificar un entorno seguro y confiable en la esfera de la banca electrónica.

Bibliografía

Abad, G. A. (2021). Análisis de la responsabilidad bancaria en casos de estafas electrónicas mediante redes sociales desde la óptica del derecho de consumo, *elDial.com,* DC2DE4

Acurio Del Pino, S. (2016). *Delitos informáticos: generalidades,* http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf.

Arias, M. P. & Müller, G. E. (2021). 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, *SJA*. 2021-211.

Banco Central de la República Argentina (9 de marzo de 2023). El BCRA actualiza las normas de riesgos de tecnología y seguridad de la información para fortalecer la ciberresiliencia de las entidades financieras, https://www.bcra.gob.ar/Noticias/BCRA-mejora-normas-tecnologia-seguridad-informacion-entidades-financieras.asp

_____ (diciembre de 2022). *Informe sobre protección a las personas usuarias de servicios financieros*. BCRA.

Banco Interamericano de Desarrollo y Organización de los Estados Americanos (2020). *Ciberseguridad riesgos, avances y el camino a seguir en América Latina y El Caribe.: Reporte Ciberseguridad 2020,* https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Barbier, E. A. (2002). *Contratación Bancaria*, Tomo I, Consumidores y usuarios, 2° Edición. Buenos Aires: Astrea.

Barreira Delfino, E. A. (2006). Cuenta corriente bancaria. Operatoria. Problemática. Abusos y responsabilidades, en María E. Kabas de Martorell (Dir.). *Responsabilidad de los bancos frente al cliente*, pp. 252-201. Santa Fe: Rubinzal- Culzoni.

Basel Committee on Banking Supervision (BCBS) (2004). *Principles for the home-host recognition of AMA operational risk capital*‖, January.

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

Camerini, M. A. (2012). Apuntes sobre los riesgos de la actividad bancaria, *Revista de Derecho Bancario y Financiero*, 7, 31-10-2012, IJ-LXVI-479.

Caramuto Martins, G. (2013). *Influencia de la Ciencia Ficción en las TIC y las Telecomunicaciones*. Trabajo Fin de Carrera/Grado. E.U.I.T. Telecomunicación (UPM) [antigua denominación], Madrid, https://oa.upm.es/20938/

Carril, M. P. (2022). Responsabilidad de las entidades bancarias ante estafas electrónicas. El deber de seguridad y prevención en el marco del contrato de consumo. *Revista Jurídica de la Universidad de San Andrés*, (13), 52-66, https://revistasdigitales.udesa.edu.ar/index.php/revistajuridica/article/view/143

Centro de Estudios de Derecho e Investigaciones Parlamentarias (CEDIP) (2022). *La Ciberseguridad: Un Estudio Comparado*. México D. F.: Cámara de Diputados LXV Legislatura.

Comité de Sistemas de Pago y Liquidación (CPSS) – Organización Internacional de Comisiones de Valores (IOSCO). (2012). *Principios aplicables a las Infraestructuras del Mercado Financiero*. Suiza: Banco de Pagos Internacionales.

Cornet, M. (2016). La culpa ¿Un factor de imputación en vías de extinción? *Revista Iberoamericana de Derecho Privado* (4) 01-12-2016, IJ-CCLI-791.

Defensoría del Pueblo de la provincia de Santa Fe (1 de enero de 2023). Estafas virtuales: el Banco de Santa Fe adoptó medidas solicitadas por la Defensoría del Pueblo. https://www.defensoriasantafe.gob.ar/articulos/estafas-virtuales-el-banco-de-santa-fe-adopto-medidas-solicitadas-por-la-defensoria-del

Dirección Nacional de Ciberseguridad (2022). *Incidentes informáticos. Informe anual de incidentes de seguridad informática registrados en el 2021 por el CERT.ar*, Argentina, febrero de 2022, pp. 2-3, https://www.argentina.gob.ar/sites/default/files/2022/02/informe_2_cert_2021_f_.pdf

Consejo Federal del Consumo (COFEDEC) (2022). *CUADERNILLO Nº2 Ciberdelitos y Estafas Digitales.* Buenos Aires: Escuela Argentina de Educación en Consumo. Dirección Nacional de Defensa del Consumidor y Arbitraje del Consumo. Secretaría de Comercio Interior, Ministerio de Economía, https://www.argentina.gob.ar/sites/default/files/cuadernillo_2_-_cofedec1.pdf

Farinati, E. N. (2009). Prácticas bancarias, dinero, banca y transferencia electrónica de fondos, en *Protección jurídica del consumidor bancario*, pp. 79-238. Buenos Aires: Ad Hoc.

Fernández Delpech, H. (2014). *Manual de Derecho informático*. Buenos Aires: Abeledo - Perrot.

Fernández, A. (2019). Internet y las nuevas formas jurídicas, sociales y punitivas. En *Era digital: delito y prevención*, Vanesa Ferrazzuolo. Libro Digital, PDF. Ciudad Autónoma de Buenos Aires: Jusbaires pp. 159-188

Fuentes, L. (2008). Malware, una amenaza de internet. *Revista Digital Universitaria*, 9 (4): pp. 2-9.

Gallasso, M. L. (2010). *La Responsabilidad Bancaria frente a fraudes cometidos por el uso de los servicios informáticos*. Tesis de Grado. Universidad Empresarial Siglo 21. Cordoba, Argentina., https://n9.cl/cev13

González-Nucamendi, A. & Solís-Rosales, R. (2012). El ABC de la regulación bancaria de Basilea. *Análisis Económico*, 27 (64), 105-139

Hernández, C. A. (2016). "El "contrato de consumo" en el contexto de la "teoría general del contrato". A propósito del código civil y comercial (expresión de una nueva estructura tipológica), *SJA* 30/03/2016, 11, JA 2016-I, AR/DOC/4158/2016.

iProUP (1 de septiembre de 2022). Entidades financieras y fintech se unen por una causa común: ¿cuál es y qué pacto firmaron?, https://www.iproup.com/finanzas/34039-fintech-acuerdo-con-entidades-financieras-por-ciberseguridad

Liendo, G. (2016). Los contratos bancarios previstos en el Código Civil y Comercial de la Nación y la protección tuitiva a favor del débil jurídico para restablecer el equilibrio en esa relación. *Ratio Iuris. Revista De Derecho,* 4(2), PAGS https://publicacionescientificas.uces.edu.ar/index.php/ratioiurisB/article/view/282

Lorenzetti, R. (2003). *Consumidores*. Santa Fe: Rubinzal – Culzoni.

_____ (2001). *Comercio electrónico.* Buenos Aires: Abeledo Perrot.

Lovece, G. I. (2016). Las relaciones de consumo. La prevención, la seguridad y el riesgo empresario, *LL* LA LEY2016-D, 549, AR/DOC/2349/2016.

Luzzi, M. (2022). *Deudas, cuidados y vulnerabilidad: interacciones de las mujeres con organizaciones financieras y no financieras en la Argentina*, Documentos de Proyectos (LC/TS.2022/59-LC/BUE/TS.2022/7). Santiago (Chile): Comisión Económica para América Latina y el Caribe (CEPAL).

Malvaso, S. G. (septiembre de 2017). El riesgo cibernético en la actividad bancaria. *Revista de Derecho Bancario y Financiero*, 36, 20-09-2017, IJ-CDLXVIII-963.

Marienhoff, M. S. (1987). *Tratado de Derecho Administrativo*. 4° Ed. Buenos Aires, Abeledo – Perrot.

Martins dos Santos, Bruna (2022). *Convenio de Budapest sobre la Ciberdelincuencia en América Latina: Un breve análisis sobre adhesión e implementación en Argentina, Brasil, Chile, Colombia y México*. https://www.derechosdigitales.org/wp-content/uploads/ESPCiberdelincuencia-2022.pdf

Mazzinghi, M. (2020). Los contratos bancarios en el nuevo Código, *RCCyC* 2015 (diciembre), 16/12/2015, 159, AR/DOC/4264/2015.

Moisset de Espanés, L. (1995). El acto ilícito y la responsabilidad civil, en *La responsabilidad: homenaje al profesor Doctor Isidoro H. Goldenberg*, Atilio Aníbal Alterini y Roberto M. López Cabana (Dir.) pp. 95-102. Buenos Aires: Abeledo-Perrot.

Organización de las Naciones Unidas (2020). *La ciberdelincuencia, en resumen*. https://www.unodc.org/e4j/es/cybercrime/module-1/keyissues/cybercrime-in-brief.html

Pizarro, D. R. (2007). *Responsabilidad civil por riesgo creado y de empresa. contractual y extracontractual*, T3. Buenos Aires: La Ley.

Porthé, L. (2008). Responsabilidad de las entidades bancarias ante el consumidor, *Lecciones y Ensayos*, 84, enero-diciembre 2008, <http://www.derecho.uba.ar/publicaciones/lye/revistas/84/09-winitzky-porthe.pdf>

Ritto, G. (2016). *Sistema de Defensa del Consumidor*. Buenos Aires: Grupo Editorial 20XII

_____ (2015). Contratos Bancarios en el Código Civil y Comercial de la Nación. *Ratio Iuris. Revista de Derecho Privado*, 3(2), 1-22.

Rivera J. C. y Medina, G. (Dir.) (2015). *Código Civil y Comercial Comentado*, Tomo III, Buenos Aires: Thomson Reuters, La Ley.

Rodríguez Romeo, P. (2 de septiembre de 2021) ¿Qué es la ingeniería social? La herramienta más utilizada por los ciberdelincuentes para cometer estafas, *Microjuris*, MJ-DOC-16154-AR | MJD16154

Rusconi, D. D. (2008). La noción de consumidor en la nueva ley, *JA Número Especial. Régimen de Defensa del Consumidor-Análisis de su reforma,* 2008-II, pág.15.

Saín, G. (2018). La estrategia gubernamental frente al cibercrimen: la importancia de políticas preventivas más allá de la solución penal, en Parada, R. y Errecaborde, J. (Comp.), *Cibercrimen y los delitos informáticos: los nuevos tipos penales en la era de Internet*, pp. 7-32. Buenos Aires: ERREIUS.

Saires, G. A. & Héctor, M. E. (2022). Juzgamiento de la obligación de seguridad de los bancos con un triple fundamento de fuentes: constitucional, legal y reglamentaria. *MJ*-DOC-16576-AR||MJD16576

Sozzo, C. G. (2015). La prevención de los daños al consumidor, en *Tratado de Derecho del Consumidor*, Gabriel Stiglitz y Carlos A. Hernández (Dir.), Tomo III, Buenos Aires: La Ley.

Stiglitz, G. (2015). Restricciones a la exoneración por causa ajena. Culpa del consumidor. Hiposuficientes. Autorización administrativa, en *Tratado de Derecho del Consumidor*, Gabriel Stiglitz y Carlos A. Hernández (Dir.), Tomo III. Buenos Aires: La Ley.

Tambussi, C. (2021). La relación de consumo en el Derecho argentino. *LEX - REVISTA DE LA FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS*, 19(27), 181-194. doi:http://dx.doi.org/10.21503/lex.y19i27.2255

Toscano, L. E. (2006). El Derecho Bancario frente a las nuevas tecnologías. Los riesgos derivados de su aplicación. Enfoque integral y práctico de la cuestión, *AR, Rev. de*

Derecho Informático, 100, nov. 2006, https://www.alfa-redi.org/sites/default/files/articles/files/toscano.pdf

Vázquez Ferreyra, R. & O. Romera (1996) La Ley de Defensa del Consumidor en los contratos bancarios a la luz de un valioso precedente judicial, *LL*, 1996- C. AR/DOC/12845/2001

Villegas, C. G. (2015). Contratos Bancarios, en *Código Civil y Comercial Comentado*, Julio César Rivera y Graciela Medina, directores, Tomo IV, Buenos Aires: Thomson Reuters, La Ley.

_____ (2005). *Contratos Mercantiles y Bancarios*. Buenos Aires: Edición del Autor.

Villegas López, A. (2018). *Aplicación de los principios de la Ingeniería del Malware al contexto del Pentesting*. Tesis de Maestría. Director: Prof. David Arroyo Guardeño. Universidad Autónoma de Madrid. Escuela Politécnica Superior.

Wajntraub, J. H. (2015). Código Civil y Comercial de la Nación Comentado. Ricardo Lorenzetti (Dir.), Tomo VI. Buenos Aires: Rubinzal - Culzoni.