DIPUTADOS
ARGENTINA

**PROYECTO DE LEY**

*La Cámara de Diputados y el Senado sancionan con fuerza de ley:*

**ARTÍCULO 1°:** Sustitúyase el nombre del Capítulo II por "INFORMACIÓN AL CONSUMIDOR Y PROTECCIÓN DE SU PERSONA", y modifícase el art. 5º de la Ley 24.240, el que queda redactado de la siguiente manera:

"Art. 5º - *Protección al Consumidor. Las cosas y servicios deben ser suministrados o prestados en forma tal que, utilizados en condiciones previsibles o normales de uso, no presenten peligro alguno para la salud o integridad física* ***y bienes*** *de los consumidores o usuarios.* ***En caso de ser utilizados de manera virtual, deben ofrecer una navegación simple, segura y eficaz****".*

**ARTÍCULO 2°:** Incorpórase a la Ley 24.240, como nuevo artículo 36 bis, el siguiente:

"Art. 36º bis – *Las* ***empresas privadas que operan por canales virtuales, incluyendo las entidades financieras (home banking),*** *están obligadas a adoptar medidas eficaces y suficientes para asegurar la identidad del usuario, junto a un sistema de alertas ante la existencia de movimientos inusuales por fuera de los patrones habituales del consumidor.*

*Asimismo, sus sitios webs deben estar diseñados según parámetros tendientes a lograr* ***la accesibilidad digital de todos los consumidores*** **."**

**ARTÍCULO 3°:** Comuníquese al Poder Ejecutivo.

Dip. Gabriela Brouwer de Koning

COFIRMANTES
Pablo Cervi
Marcela Antola
Danya Tavela
Margarita Stolbizer
Héctor Antonio Stefani
Hernán Lombardi
Ana Clara Romero
Carlos Raúl Zapata
Rodrigo de Loredo

**FUNDAMENTOS**

Señor Presidente:

Introducción

En primer lugar, proponemos cambiar el nombre del Capítulo II por “Información al Consumidor y Protección de su Persona”, porque al utilizarse el concepto de *Persona, éste* resulta abarcativo de una mayor protección al consumidor, tanto de su integridad física (salud) como de sus bienes, en tanto el patrimonio resulta uno de los atributos de la personalidad.

Repárese que con la virtualidad se observa un exponencial crecimiento de los denominados ciberdelitos, este tipo de estafas y defraudaciones patrimoniales viene creciendo en nuestro país y sus modalidades más comunes son la suplantación de identidad, el fraude y el robo de cuentas bancarias.

En el ámbito del servicio bancario, desde hace un tiempo se ha instaurado la utilización de entornos digitales, de manera tal que el uso de la tecnología en los productos y servicios financieros viene creciendo significativamente en los últimos años. La gran mayoría de los bancos hace años que ofrecen a sus clientes Apps (aplicaciones móviles) y home banking para realizar la mayor parte de las operaciones.

Ante este nuevo escenario, el aumento del uso de los entornos digitales de las entidades bancarias y financieras, también trajo aparejado el incremento de los ciberdelitos, una de las maniobras de estafa más comunes consiste en gestionar un crédito vía online a nombre de la víctima y una vez depositado el dinero en su home banking, resulta apropiado por un tercero de manera fraudulenta (“phishing”).

El "phishing" es un término utilizado por los especialistas en informática para denominar una conducta ilícita que puede ser encuadrada en el campo de las denominadas estafas informáticas y que se comete mediante el uso de la ingeniera social en la que existe algún tipo de manipulación con un anzuelo -premio y una pesca- entrega de claves.

Se ha afirmado -en posición que compartimos- que “el sistema informático que maneja el ingreso remoto de clientes al sistema bancario es una cosa riesgosa” (CNCom, Sala D, 15/5/2008, “Bieniauskas, Carlos c/ Banco de la Ciudad de Buenos Aires”, elDial.com - AA4927).

En función de ello, las entidades financieras deben tener la obligación expresa de desplegar medidas suficientes y adecuadas para dar cumplimiento efectivo a su deber de seguridad en el entorno digital utilizado por los usuarios.

Bajo el principio del régimen consumeril que consagra una obligación de seguridad a cargo de los proveedores, entendemos que los bancos deben proporcionar una plataforma tecnológica moderna que provea confiabilidad, integridad y disponibilidad de la información en una red consolidada y segura. En otras palabras, los bancos deben asegurar a sus usuarios la seguridad de estos entornos digitales, debiendo desplegar herramientas de ciberseguridad.

Advierta Sr. Presidente que el presente proyecto refleja y se cohonesta con recientes precedentes jurisprudenciales en la materia, confrontar por ejemplo los autos: “Suárez Daniel Ricardo C/ Banco de la Provincia de Buenos Aires S/ Nulidad de Contrato Digital (Expte: LP - 36125 - 2020), de fecha 14/02/22 del Juzgado Civil y Comercial N° 19 de La Plata.

En el fallo referenciado la Sra. Jueza interviniente verificó y analizó si había incumplimiento por parte de una entidad bancaria con las medidas indispensables para otorgar seguridad informática a las transacciones. El primer interrogante en el juzgamiento radicó en establecer cuál fue la actuación desplegada por el banco demandado.

En este sentido el perito informático de la causa dictaminó que la demandada (banco), si bien cumplía con las medidas de concientización, capacitación, integridad y registro y gestión de incidentes, no cumplía con el monitoreo y control. Este último es un proceso relacionado con la recolección, análisis y control de eventos ante fallas, indisponibilidad, intrusiones y otras situaciones que afecten los servicios ofrecidos por los canales electrónicos, y que puedan generar un daño eventual sobre la infraestructura y la información. Pudo determinar que surgían del log de transacciones operaciones en las que se involucraban montos importantes que no recibieron el tratamiento que correspondía por su carácter de sospechosas o potencialmente fraudulentas.

Citamos más jurisprudencia:

"*En el contexto descripto, los bancos debieron tomar medidas a fin de brindar a sus clientes un uso seguro de los servicios ofrecidos. Es que la obligación de seguridad se extiende a esos servicios digitales, lo que impone que los bancos deben proveer la gestión, implementación y control de los riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras, de manera tal que su utilización sea segura parar los usuarios*." (Cfr. Autos: "Urquía, Nicolás Martín C/ Banco Bbva Argentina S.A. - Abreviado - Otros - Expte. 10176944", Juz. C.C. 1° Inst. y 3° Nom. Sec. N° 6 de la ciudad de San Francisco, Pcia. de Córdoba, 06.02.22).

*"Los bancos, como proveedores profesionales en la actividad bancaria, también tienen este deber de seguridad. En este sentido, se ha dicho que el banco acepta cuidar los fondos de una inmensa masa de personas que, como es obvio, no tienen todas el mismo nivel cultural, ni idénticas capacidades, habilidades o situaciones personales, por lo que él no puede ignorar que el acceso a sea gigantesca fuente de recursos monetarios que le traen lucro, tiene como correlato lógico su obligación de hacerse cargo de atender a todos, llevando al límite los arbitrios posibles para minimizar los riesgos a los que habrán de estar expuestos los usuarios."* (Conf. CNCom, Sala C, 24/5/2016, "H., M. C. c/ Banco Ciudad de Buenos Aires - Ordinario).

"*Consumo, publicidad y crédito constituyen un triángulo que retroalimenta el sistema de la sociedad de consumo: la creación y fomento de necesidades se desarrollan por la publicidad, la moda y las prácticas comerciales en general, en tanto que la facilitación al consumo viene de la mano con la generalización y ampliación de las modalidades de financiación.*" (Stiglitz, Gabriel, "La protección del consumidor de servicios financieros y bursátiles", TR LA LEY AR/DOC/29921/2015).

Además, las disposiciones de la Ley de Defensa del Consumidor se deben integrar al nuevo marco legal de derecho privado, todo ello en una interpretación "sistémica y coherente" (art. 2° Cód. Civil y Comercial) con los postulados protectorios de los consumidores receptados por la Constitución Nacional en su art. 42°; arts. 7°, 1094° ss. y cc. del CCCN; resol. 36/19 del Mercosur.

Los arts. 1384° a 1389° del Código Civil y Comercial de la Nación establecen que las normas del sistema protectorio del consumidor resultan aplicables a los contratos bancarios con consumidores y usuarios.

Y en este moderno contexto, además se observa la existencia de consumidores "hipervulnerables" en razón de su edad, género, estado físico o mental, o por circunstancias sociales, económicas, étnicas y/o culturales, que provocan especiales dificultades para ejercer con plenitud sus derechos como consumidores.

Los adultos mayores cuentan con la especial protección de la Convención Interamericana sobre la Protección de los Derechos Humanos de las Personas Mayores, aprobada por la Ley N° 27.360 (9/5/2017). El objeto de la Convención es promover, proteger y asegurar el reconocimiento y el pleno goce y ejercicio, en condiciones de igualdad, de todos los derechos humanos y libertades fundamentales de la persona mayor, a fin de contribuir a su plena inclusión, integración y participación en la sociedad.

El último relevamiento sobre Accesibilidad digital para personas mayores: portales bancarios, realizado por el *Instituto de Género y Promoción de la Igualdad*, retoma conclusiones del informe *Personas Mayores, Vivencias y dificultades en pandemia* que señala el escaso vínculo que tuvieron las personas mayores con las nuevas tecnologías de la información y la comunicación, cuando las mediaciones virtuales y digitales ocuparon la vida cotidiana de todas las personas. El acceso a la conectividad, los dispositivos tecnológicos y el manejo de éstos, dejó en evidencia la brecha digital generacional y las barreras funcionales propias de la edad. Además, según dicho informe solo un 26% de los bancos, disponen de un canal de asistencia o consulta en línea, a través de un sistema automático de mensajería, o un número telefónico de WhatsApp para interactuar con la entidad.

Por su parte, el Banco Central de la República Argentina (BCRA), como autoridad de contralor, ha emitido una serie de normas referidas al deber de seguridad y diligencia que deben asumir las entidades bancarias, en lo que concierne al resguardo de la información de los clientes y usuarios, particularmente en las operaciones efectuadas a través de medios remotos, a saber: 1) Comunicación "A" N° 7249, de fecha 31/03/2021, 2.1.: "Los usuarios de servicios financieros tienen derecho, en toda relación de consumo, a: la protección de su seguridad e intereses económicos (...)"

2) Comunicación "A" N° 7175, artículo 2.3. Responsabilidades de los participantes; 2.3.1.: Las entidades participantes, ya sea en calidad de originantes o receptoras y los PSPs deberán arbitrar los mecanismos de seguridad apropiados dentro de su competencia para asegurar la transmisión y recepción de las transacciones, como así también tendrán las siguientes responsabilidades: (...) 2.3.2.8: Ofrecer herramientas de mitigación de fraude a sus participantes (...) 2.3.3.5: Utilizar herramientas de mitigación de fraude que permitan identificar patrones sospechosos, y alertar a los usuarios.

3) Comunicación "A" N° 7072, artículo 2.2.2.11: "Política "conozca a su cliente": recaudos especiales a tomar de manera previa a la efectivización de una transferencia, a los fines de continuar

con la política de minimizar el riesgo, particularmente con respecto a las cuentas que presenten algunas de las siguientes características: Cuentas de destino que no hayan sido Expediente SAC 10176944 - Pág. 12 / 99 - Nº Res. 1 previamente asociadas por el originante de la transferencia a través de cajeros automáticos, en sede de la entidad financiera o por cualquier otro mecanismo que ella considere pertinente; Cuentas de destino que no registren una antigüedad mayor a 180 días desde su apertura; Cuentas que no hayan registrado depósitos o extracciones en los 180 días anteriores a la fecha en que sea ordenada la transferencia inmediata. En caso de no producirse la justificación del movimiento en el término previsto, la entidad receptora deberá proceder al rechazo de la transferencia.

4) Comunicación "A" Nº 6664, artículo 1.1.1., define al "Usuario de Servicios Financieros", como "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 servicios ofrecidos por los sujetos obligados que se enuncian en el punto 1.1.2., como a quienes de cualquier otra manera están expuestos a una relación de consumo con tales sujetos", adicionando en su artículo 2.1. que "los usuarios de servicios financieros tienen derecho, en la relación de consumo respectiva, a: - la protección de su seguridad e intereses económicos (...)". De dicha normativa se desprende que, como principal sujeto obligado a custodiar la seguridad e intereses económicos, es la entidad bancaria, en este caso, BBVA.

5) Comunicación "A" Nº 6878, artículo 3.8.5, dispone "(...) *Las entidades deberán prestar atención al funcionamiento de las cuentas con el propósito de evitar que puedan ser utilizadas en relación con el desarrollo de actividades ilícitas"*, agregando que *"deberán adoptarse normas y procedimientos internos a efectos de verificar que el movimiento que se registre en las cuentas guarde razonabilidad con las actividades declaradas por los clientes*". Asimismo, destaca en reiteradas oportunidades, la "implementación de mecanismos de seguridad informática que garanticen la genuinidad de las operaciones". Ello, de conformidad con los artículos 1.6.2, 1.6.3, 1.7.2, 1.7.3 y 3.4.5. de la Comunicación citada en el presente párrafo.

6) Comunicación "A" Nº 6017, concerniente a los "REQUISITOS MÍNIMOS DE GESTIÓN, IMPLEMENTACIÓN Y CONTROL DE LOS RIESGOS RELACIONADOS Expediente SAC 10176944 - Pág. 13 / 99 - Nº Res. 1 CON TECNOLOGÍA INFORMÁTICA, SISTEMAS DE INFORMACIÓN Y RECURSOS ASOCIADOS PARA LAS ENTIDADES FINANCIERAS", se destaca en el artículo 6.3.2.1 que las "Las entidades deben desarrollar, planificar y ejecutar un plan de protección de sus activos, procesos, recursos técnicos y humanos relacionados con los Canales Electrónicos bajo su responsabilidad, basado en un análisis de riesgo de actualización periódica mínima anual, en su correspondencia con la Matriz de Escenarios y en los requisitos técnico operativos detallados en los puntos 6.7. y subsiguientes", enumerando seguidamente, una serie de funciones y tareas relacionadas con los procesos estratégicos de seguridad para sus Canales Electrónicos, de conformidad con lo que surge del artículo 6.3.2.2. Entre ellas, se ordena a las entidades "(...) contar con un programa de concientización y capacitación de seguridad informática anual, medible y verificable, cuyos contenidos contemplen todas las necesidades internas y externas

en el uso, conocimiento, prevención y denuncia de incidentes, escalamiento y responsabilidad de los Canales Electrónicos con los que cuentan (...) adquirir, desarrollar y/o adecuar los mecanismos implementados para la verificación de la identidad y privilegios de los usuarios internos y externos, estableciendo una estrategia basada en la interoperabilidad del sistema financiero, la reducción de la complejidad de uso y la maximización de la protección del usuario de servicios financieros (...) garantizar un registro y trazabilidad completa de las actividades de los Canales Electrónicos en un entorno seguro para su generación, almacenamiento, transporte, custodia y recuperación", entre otras (cfme. art. 6.3.2.2.). Ello así, define "Concientización y Capacitación (CC)", como aquel "Proceso relacionado con la adquisición y entrega de conocimiento en prácticas de seguridad, su difusión, entrenamiento y educación, para el desarrollo de tareas preventivas, detectivas y correctivas de los incidentes de seguridad en los Canales Electrónicos" y "Control de Acceso (CA)", como el "Proceso relacionado con la evaluación, desarrollo e implementación de medidas de seguridad para la protección de la identidad, mecanismos de autenticación, segregación de roles y funciones y demás características del acceso a los Canales Expediente SAC 10176944 - Pág. 14 / 99 - Nº Res. 1 Electrónicos" (cfme. arts. 6.2.1. y 6.2.2., respectivamente). Posteriormente, dicha Comunicación, en su artículo 6.7.1., dispone que, "los contenidos del programa de [concientización y capacitación] deben incluir: técnicas de detección y prevención de apropiación de datos personales y de las credenciales mediante ataques de tipo 'ingeniería social', 'phishing', 'vishing' y otros de similares características", mientras que en el artículo 6.7.4., en lo referente a los mecanismos de monitoreo y control de las entidades bancarias, resalta que, "las entidades deben disponer de mecanismos de monitoreo transaccional en sus [canales electrónicos], que operen basados en características del perfil y patrón transaccional del cliente bancario, de forma que advierta y actúe oportunamente ante situaciones sospechosas en al menos uno de los siguientes modelos de acción: a. Preventivo. Detectando y disparando acciones de comunicación con el cliente por otras vías antes de confirmar operaciones. b. Reactivo. Detectando y disparando acciones de comunicación con el cliente en forma posterior a la confirmación de operaciones sospechosas. c. Asumido. Detectando y asumiendo la devolución de las sumas involucradas ante los reclamos del cliente por desconocimiento de transacciones efectuadas".

En apretada síntesis, las entidades financieras, definidas por Ley Nº 21.526, deben adoptar una conducta en la cual ponderen los riesgos previsibles, con el objeto de proteger suficientemente a los usuarios de eventuales estafas.

Las entidades bancarias deben contar con un sistema informático de protección suficiente para prevenir e impedir maniobras fraudulentas, en base a la previsibilidad y normalidad en la prestación del servicio y en el uso de las cosas.

Frente a operatorias inusuales, deben generar alertas para detectar este tipo de actos irregulares e infrecuentes, resultando esperable que una entidad bancaria adopte una conducta en la cual pondere los riesgos previsibles, con el objeto de proteger a los usuarios.

La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de una organización (pública o privada) y a los usuarios en el ciberentorno. A su vez, todo sistema de ciberseguridad debe propiciar la protección de los siguientes ítems: la confidencialidad de los datos: impedir la divulgación de información a personas o sistemas no autorizados; la integralidad: lo que importa decir que los datos personales allí almacenados no puedan ser modificados o borrados por personal autorizado o no (intrusos/hacker), por un mecanismo extraño (virus), etcétera; la disponibilidad: lo cual significa que los datos personales deben encontrarse a disposición de quienes correspondan acceder a ellos, ya sean personas autorizadas, procesos o aplicaciones, siempre y cuando se respeten los protocolos y mecanismos de seguridad predispuestos con antelación, los cuales deben, por ende, estar desempeñándose correctamente. Para que opere tal protección la ciberseguridad deberá contar con fases de prevención, localización y reacción ante la amenaza (VANINETTI, Hugo A., La ciberseguridad como política de Estado. Estrategia Nacional de Ciberseguridad. Decreto 829/2019. Protección de los datos e intimidad personal, Sup. Esp. LegalTechII 2019 (noviembre), 103, TR LALEY AR/DOC/3582/2019).

Por las razones expuestas, consideramos necesario modificar la Ley de Defensa del Consumidor, microsistema jurídico que significó un gran avance en la legislación existente, por cuanto reconoció en favor de los usuarios o consumidores un conjunto de valiosos derechos, algunos de contenido económico y otros de raigambre extrapatrimonial, y que a nuestro entender en su proceso evolutivo debe continuar ampliando el abanico de tutelas consagradas por la norma del art. 42º de nuestra Carta Magna.

Dip. Gabriela Brouwer de Koning

COFIRMANTES
Pablo Cervi
Marcela Antola
Danya Tavela
Margarita Stolbizer
Héctor Antonio Stefani
Hernán Lombardi
Ana Clara Romero
Carlos Raúl Zapata
Rodrigo de Loredo


DIPUTADOS
ARGENTINA