PROYECTO DE LEY

El Senado y la Cámara de Diputados de la Nación Argentina sancionan con fuerza de ley:

Prevención, Persecución y Protección frente al Cibercrimen Financiero: modificación de la Ley 26.637 para la incorporación de delitos informáticos, evidencia digital y cadena de custodia

Artículo 1° – Sustitúyese el artículo 2º de la Ley N.º 26.637, el que quedará redactado de la siguiente forma:

Artículo 2°. - Las entidades financieras y prestadoras de servicios pago (PSP) y otras entidades que defina el BCRA, deberán implementar medidas de seguridad física y digital, según corresponda, destinadas a proteger a las personas, los valores y la información sensible dentro de sus instalaciones, así como a prevenir delitos convencionales y cibernéticos.

a) derogase la prohibición generalizada del uso de teléfonos móviles dentro de las dependencias bancarias.

b) derogase la utilización de inhibidores de señal dentro de las entidades bancarias.

c) Las entidades deberán establecer mecanismo para la detección, monitoreo y prevención de delitos informáticos y cibernéticos en el ámbito financiero.

d) Los delitos informáticos a prevenir y reprimir en el ámbito de los servicios financieros digitales comprenden, de manera taxativa, los siguientes tipos penales previstos en el Código Penal de la Nación:

- Acceso ilegítimo a sistemas o datos informáticos (arts. 153 y 153 bis),
- Violación de secretos y privacidad (arts. 155, 157 y concordantes),
- Daño o sabotaje informático (arts. 183, 184 y 185),
- Defraudaciones informáticas y manipulación de sistemas digitales (art. 173 inciso 16),
- Amenazas y extorsión mediante medios digitales (arts. 149 bis y 168),
- Usurpación de identidad digital y uso ilegítimo de datos personales sensibles (arts. 172, 173 y 174, según el caso),
- Asociación ilícita para cometer delitos informáticos (arts. 210 y 210 bis),
- Captación o manipulación digital de imágenes o voces con fines de fraude o suplantación (art. 226 ter),
- Y toda otra conducta delictiva que afecte la confidencialidad, integridad o disponibilidad de sistemas, redes, datos o servicios, incluyendo el phishing, el ransomware, el malware financiero, el uso malicioso de tecnologías deepfake o de inteligencia artificial generativa, y la manipulación o sustracción de datos biométricos, cuando encuadren en figuras típicas penales vigentes.

e) El Poder Judicial y las fuerzas de seguridad deberán regirse por una normativa específica, clara y actualizada sobre recolección, conservación, trazabilidad, análisis técnico y validación procesal de evidencia digital, bajo estricto cumplimiento de los principios de legalidad, cadena de custodia y control jurisdiccional.

Artículo 2° – Comuníquese al Poder Ejecutivo.

Firmante: Gerardo Milman.

FUNDAMENTOS

Señor presidente:

I. Introducción: de la violencia física a la ciber-transaccionalidad

Cuando el Congreso sancionó la Ley 26.637 en 2010, la amenaza predominante sobre las sucursales bancarias eran las denominadas "salideras bancarias". En ese contexto, la prohibición absoluta de utilizar teléfonos móviles buscaba impedir la inteligencia previa y la coordinación "en vivo" de los delincuentes dentro y fuera de la entidad.

Quince años después, la escena cambió radicalmente: las operaciones financieras se migraron a plataformas digitales y el teléfono inteligente se transformó en llave de acceso a la identidad y al dinero del cliente. Mantener un veto generalizado a su uso dentro de la sucursal implica hoy dificultades operativas que ya no se justifican en términos de seguridad.

II. La revolución digital de la banca argentina

El Banco Central de la República Argentina (BCRA) reporta que en el segundo trimestre de 2024 el 73,8 % de las personas humanas con cuenta registró al menos una operación digital —transferencia, pago o billetera—, un salto de más de 30 puntos respecto de 2019.

En términos de acceso, la población adulta presenta hoy una penetración del 102,4 % (más de una cuenta por persona), cifra que refleja la superposición de cuentas bancarias y virtuales.

Estas estadísticas no describen solo un cambio cuantitativo: revelan la consolidación del móvil como canal principal. El 2024 cerró con 38,3 millones de argentinas y argentinos titulares de CBU y 27,5 millones de CVU, con un crecimiento de las billeteras virtuales que quintuplica al de las cuentas tradicionales.

III. El teléfono como segundo-factor y credencial de identidad

Los factores de autenticación basados en "soft-token", contraseñas dinámicas y biometría se generan, validan o almacenan en el dispositivo móvil. Sin ese segundo factor la operación simplemente no se completa.

Incluso trámites presenciales —apertura de caja de ahorro, gestión de clave CBU, retiro de divisas o validación KYC— exigen al cliente "levantar" la app, aceptar un push o mostrar un QR generado en pantalla. Obligar al usuario a depositar su teléfono en lockers o bolsas de Faraday provoca colas, frustración y —paradójicamente— tentaciones de violar la norma dentro del salón.

IV. Persistencia normativa y brecha regulatoria

Pese a aquella evolución, el flujo operativo de las sucursales continúa regido por la vieja directiva. La norma de medidas mínimas de seguridad del BCRA reafirma explícitamente "la prohibición del uso de telefonía celular prevista por el inciso c) del artículo 2° de la Ley 26.637".

Este anacronismo genera choques cotidianos entre usuarios y personal bancario y, sobre todo, expone a la institución a litigios por denegación injustificada de servicios o trato inequitativo (arts. 42 y 43 de la Constitución Nacional; Ley 24.240 de Defensa del Consumidor).

V. Riesgos reales y riesgos desplazados

La amenaza que justificó la prohibición (vigilancia disimulada de cajas y coordinación de asaltos) mutó gracias a la videovigilancia HD, la marcación electrónica de billetes y el blindaje de tesoros. En cambio, el delito se trasladó al hurto de celulares: hoy representa el 27 % del total de robos en Argentina y se consuma mayoritariamente en la vía pública.

La paradoja es evidente: el dispositivo cuya presencia se teme dentro del banco es, fuera de él, el botín más buscado, vector de fraudes y extorsiones a posteriori.

Permitir su uso en la sucursal reduce la necesidad de que el cliente despliegue credenciales fuera de un ámbito protegido y monitoreado.

VI. Benchmarks internacionales

Unión Europea: la Directiva PSD2 obliga desde 2019 a implementar "autenticación reforzada" (SCA) con al menos dos factores —uno de los cuales, habitualmente, es el móvil— incluso dentro de la sucursal.

Estados Unidos: la Federal Financial Institutions Examination Council (FFIEC) recomienda permitir el uso de dispositivos propios bajo esquemas "bring-your-own-device controlado", con segmentación Wi-Fi y registro de MAC.

Brasil: la Resolución 4.471/2016 del Banco Central autoriza expresamente el móvil como medio de firma electrónica presencial.
El denominador común es la habilitación condicionada y monitoreada, no la supresión categórica.

VII. Nuevos delitos en la era digital: mutación del riesgo bancario Delitos informáticos y marco penal aplicable

Este proyecto incorpora de forma taxativa y expresa el catálogo de ciberdelitos que deben ser prevenidos, monitoreados y denunciados por las entidades financieras. La base normativa está contenida en los siguientes artículos del Código Penal de la Nación:

- Art. 153 y 153 bis: Acceso ilegítimo a sistemas informáticos o comunicaciones privadas.

- Art. 153 ter y 155: Revelación y uso de datos personales obtenidos ilícitamente.

- Art. 173, inc. 16: Fraude informático o manipulación digital con perjuicio económico.

- Art. 183 y 184: Daños a sistemas o datos mediante software malicioso.

- Art. 197: Perturbación de sistemas de comunicación esenciales.

Asimismo, se extiende la tipificación a nuevas formas de criminalidad digital, como:

- Suplantación de identidad mediante deepfake o IA generativa.

- Ransomware y secuestro de datos con fines extorsivos.

- Manipulación de bases de datos biométricos.

- Uso delictivo de canales de pago digital para el blanqueo de activos.

La responsabilidad preventiva de las entidades bancarias se activa no solo por omisión o negligencia en su deber de custodia de los datos, sino también por falta de protocolos frente a incidentes, como lo exige la Ley 25.326 y el principio de "accountability" del régimen internacional de protección de datos personales.

La irrupción masiva de tecnologías digitales en la vida cotidiana no solo transformó la operatoria financiera, sino que también reconfiguró la morfología del delito. Las amenazas que enfrentan hoy los usuarios bancarios no se materializan en las denominadas "salideras bancarias" sino más bien en las formas sofisticadas de fraude digital, suplantación de identidad, ingeniería social, phishing, vishing, smishing, o el control remoto de dispositivos a través de malware o troyanos bancarios.

Según reportes de la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI), el 2023 cerró con un incremento del 245 % en denuncias por delitos informáticos relacionados con accesos no autorizados a cuentas bancarias y billeteras digitales. Buena parte de estas estafas se concretan en contextos donde el usuario se ve obligado a operar sin acompañamiento técnico, sin entorno seguro y, muchas veces, sin entender del todo lo que está haciendo. Permitir el uso controlado del teléfono móvil dentro de la entidad bancaria no sólo facilita la operación, sino que protege al cliente en el momento más crítico del proceso: la validación final.

Incluso, el hurto o robo de celulares —una de las modalidades delictivas más frecuentes— ha mutado su propósito: ya no se trata de comercializar el dispositivo en el mercado negro, sino de acceder a las cuentas bancarias del titular a través de sus apps sin protección o de SMS con códigos temporales. Este escenario refuerza la necesidad de que las transacciones delicadas se completen dentro del perímetro de seguridad

física y lógica que provee la entidad bancaria, y no en soledad, bajo presión o exposición en la calle.

En suma, la criminalidad financiera del siglo XXI exige un rediseño integral de las barreras de protección. La tecnología no es el enemigo: es la herramienta indispensable para mitigar el riesgo, siempre que se use bajo estándares razonables, con supervisión institucional y dentro de un marco normativo que entienda que la seguridad real ya no se mide en blindaje físico, sino en inteligencia digital, prevención activa y trazabilidad de las operaciones.

VIII. La Evidencia Digital y la Cadena de Custodia

En el nuevo ecosistema delictivo digital, la evidencia ya no se encuentra en objetos físicos fácilmente asegurables, sino en registros intangibles y dinámicos: metadatos, registros de actividad en redes, trazas de navegación, mensajes encriptados, patrones biométricos, inteligencia artificial generativa, entre otros. Por ello, se vuelve imprescindible que tanto el Poder Judicial como las fuerzas de seguridad cuenten con un marco normativo claro, actualizado y tecnológicamente viable para la recolección, conservación, trazabilidad y validación de evidencia digital. Esta normativa debe asegurar garantías procesales y derechos constitucionales, pero también permitir actuar con rapidez ante la volatilidad de la información digital. La ausencia de estándares claros expone a nulidades, arbitrariedades y fallos judiciales contradictorios, debilitando la persecución penal y generando inseguridad jurídica.

IX. Continuidad normativa y coherencia legislativa

Cabe destacar que la Ley N.º 26.637 —cuyo artículo 2° hoy se propone modificar— fue de mi autoría en mi calidad de legislador nacional. En su momento, la norma fue producto de un profundo diagnóstico sobre

las condiciones de inseguridad que afectaban a entidades bancarias, clientes y trabajadores en un contexto donde el delito violento y el uso de celulares como herramienta de logística criminal eran una amenaza real.

Sin embargo, como autor de aquella ley, me siento también en la obligación institucional y política de actualizarla frente al nuevo paradigma de amenazas y desafíos tecnológicos que impone la era digital. La modificación que proponemos no altera el espíritu original de proteger al usuario bancario, sino que lo adapta a una realidad operativa distinta, más compleja y dinámica, donde la seguridad ya no puede basarse exclusivamente en inhibiciones físicas, sino en el uso controlado de herramientas digitales, bajo estándares técnicos y criterios de razonabilidad.

Esta continuidad legislativa no solo expresa un compromiso con la mejora constante del sistema normativo, sino que además refuerza la legitimidad de la reforma propuesta, ya que parte del reconocimiento explícito de que toda ley, por buena que sea, debe revisarse a la luz de su eficacia en el tiempo, la evolución social, los cambios tecnológicos y los nuevos modos delictivos.

X. Inclusión financiera y cohesión generacional

El 84 % de las nuevas cuentas de 2024 fue abierta por personas menores de 30 años, nativas digitales que ubican al smartphone en el centro de su vida económica y social.

Impedirles utilizar la herramienta esencial para verificar su identidad equivale a erigir una barrera generacional contraria a la "igualdad real de oportunidades" que ordena el art. 75 inciso 23 de la Constitución. La reforma alinea la norma con las políticas de inclusión que el propio BCRA impulsa en su "Informe de Inclusión Financiera" y con los compromisos

asumidos por la Argentina en el G20 Global Partnership for Financial Inclusion.

XI. Arquitectura de seguridad propuesta

- Monitoreo CCTV HD focalizado sobre el área de uso para desalentar capturas ilícitas de terceros.

- Cartelería visible que explique la norma al cliente, obligación que el proyecto introduce como nuevo inciso d).

- Este enfoque "zero-trust/need-to-use" reduce el vector de riesgo sin sacrificar la agilidad operativa.

XII. Rol del BCRA como autoridad técnica

El proyecto otorga al BCRA un plazo de 60 días para emitir la reglamentación, previo proceso de consulta no vinculante con las entidades financieras, específica sobre:

- protocolos de ciberseguridad y trazabilidad;

- estándares mínimos de encriptado extremo a extremo en las apps;

- interoperabilidad con sistemas de autenticación biométrica;

- mecanismos o procesos de los bancos para bloquear cuentas o credenciales para detener cualquier fraude en curso.

- Acceso e intercambio de información online de los cuits asociados a maniobras fraudulentas.

- Protocolos standarizados para la gestión de recupero de fondos frente a eventos de fraude entre entidades.

La autoridad monetaria ya cuenta con experiencia regulatoria en la materia (p.ej., Comunicación "A" 7837/2023 sobre autenticación digital reforzada), de modo que la delegación resulta técnica, necesaria y conforme al art. 76 CN.

XIII. Impacto económico y sistémico

Para la entidad y para el sistema: se reducen costos asociados a la provisión de tokens físicos —dispositivos que requieren logística, mantenimiento y reposición— y se acorta el tiempo de atención en ventanilla y en otras posiciones.

Se fomenta la utilización de identidades digitales robustas, se acelera la trazabilidad de operaciones en moneda local (promoviendo la desmaterialización de efectivo) y se fortalece el ecosistema Fintech-banca tradicional.

Todo esto redundante en un mejor servicio a los usuarios, lo que alienta la formalización de actividades.

XIV. Conclusión

Modernizar la Ley 26.637 no significa renunciar a la seguridad; significa actualizar la estrategia defensiva para que acompañe la evolución tecnológica que ya es cotidiana en la economía argentina. Cada cliente que debe retirarse de la fila para autorizar un token fuera de la sucursal

experimenta el rezago regulatorio en carne propia. Cada banco que invierte en ciberseguridad avanzada.

La reforma propuesta restablece la proporcionalidad, fortalece la inclusión y alinea la legislación argentina con los más altos estándares internacionales.

Por todo lo expuesto, solicitamos a los señores y señoras legisladores acompañar con su voto afirmativo este proyecto.

Firmante: Gerardo Milman.