PROYECTO DE LEY

El Senado y la Cámara de Diputados sancionan con fuerza de ley…

LEY DE PREVENCIÓN, SANCIÓN Y TRAZABILIDAD DE CIBERFRAUDES

CAPÍTULO I – DISPOSICIONES GENERALES

Artículo 1°. Objeto. La presente ley tiene por objeto prevenir, sancionar y permitir la trazabilidad de los fraudes cometidos mediante el uso de medios digitales, electrónicos, redes informáticas o plataformas tecnológicas, adaptando la legislación penal vigente, estableciendo medidas de seguridad obligatorias y promoviendo la cooperación entre entidades públicas y privadas.

Artículo 2°. Ámbito de aplicación y Sujetos Comprendidos. Quedan alcanzadas por esta ley todas las personas humanas o jurídicas, públicas o privadas, que participen en la provisión de servicios financieros, bancarios, de pagos digitales, comercio electrónico o cualquier otra actividad donde intervengan datos sensibles, instrumentos de pago electrónicos o fondos digitales.

CAPÍTULO II – OBLIGACIONES DE SEGURIDAD PARA ENTIDADES Y PLATAFORMAS

Artículo 3°. Sistema Chip & PIN. Los sujetos alcanzados por la presente deberán implementar sistemas de autenticación dual "Chip & PIN" y/o la tecnología que en el futuro los mejore o reemplace, para transacciones presenciales o remotas que superen el monto que determine el Banco Central de la República Argentina, o en caso de operaciones reiteradas con la misma tarjeta.

La reglamentación establecerá excepciones fundadas y protocolos específicos que resulten de aplicación.

Artículo 4°. Seguridad en terminales de cobro y plataformas. Las terminales de punto de venta, plataformas de pago en línea y aplicaciones móviles deberán incorporar mecanismos de verificación biométrica o autenticación de múltiples factores en operaciones que, por su frecuencia, monto o patrones detectados, indiquen riesgo elevado de fraude.

Asimismo, en el caso de transferencias digitales deberán advertir de modo visible e inconfundible con la leyenda "posible destino fraudulento" cuando el destinatario posea mas de un reclamo en la base de la plataforma digital.

CAPÍTULO III – TRAZABILIDAD DIGITAL Y USO DE IP

Artículo 5°. Identificación técnica de operaciones. Las direcciones IP, metadatos, logs de sesión, dispositivos utilizados y otros identificadores técnicos de operaciones financieras, serán considerados datos relevantes a efectos de la investigación penal de ciber fraudes, y podrán ser requeridos judicialmente a entidades financieras, proveedores de servicios digitales o empresas de telecomunicaciones.

Artículo 6°. Uso de VPN o mecanismos de anonimato. El uso de tecnologías que oculten la dirección IP real no impedirá la responsabilidad penal ni eximirá a los intervinientes de colaborar con la trazabilidad técnica. Su empleo, en el contexto de fraude, podrá ser considerado agravante. La recolección de estos datos, bajo orden judicial, no constituirá violación del derecho a la privacidad.

CAPÍTULO IV – REGISTRO NACIONAL Y RÉGIMEN SANCIONATORIO

Artículo 7°. Autoridad de aplicación. El Banco Central de la República Argentina será la autoridad de aplicación de esta ley. Tendrá a su cargo la emisión de normas técnicas, supervisión del cumplimiento y aplicación de sanciones administrativas por infracciones a las obligaciones establecidas en esta ley.

Asimismo, ante la obsolescencia de las tecnologías comprendidas en la presente, la autoridad de aplicación se encuentra facultada para emitir las normas reglamentarias que resultaran necesarias para determinar la plena vigencia y aplicabilidad del presente marco normativo.

Artículo 8°. Registro Nacional de Incidentes de Ciber fraude. Créase el Registro Nacional de Incidentes de Ciber fraude en el ámbito de la central de información del Banco Central de la República Argentina, el cual será de acceso público y actualizado en tiempo real únicamente en lo relativo a estadísticas generales, patrones, alertas y medidas preventivas.

Los datos técnicos sensibles tales como direcciones IP, logs de sesión, metadatos u otros identificadores que permitan la individualización de personas físicas o jurídicas, sólo podrán ser consultados por las autoridades judiciales, el Ministerio Público Fiscal, la Unidad de Información Financiera y otros organismos competentes conforme lo determine la reglamentación.

Los sujetos comprendidos, deberán reportar todos los eventos relevantes dentro de las cuarenta y ocho (48) horas de detectados.

El registro contendrá estadísticas, patrones, alertas y medidas de respuesta, así como los IP desde los cuales se cometieron las operaciones fraudulentas.

La Autoridad de Aplicación podrá incluir información adicional a los fines de garantizar una efectiva aplicación del presente marco normativo.

CAPÍTULO V – REFORMAS AL CÓDIGO PENAL Y LEYES COMPLEMENTARIAS

Artículo 9°. Incorporación al Código Penal. Incorpórese como artículo 173 bis del Código Penal de la Nación el siguiente texto:

"Artículo 173 bis: Será reprimido con prisión de tres (3) a diez (10) años el que, mediante la manipulación informática, la obtención indebida de credenciales digitales, el uso de tarjetas falsificadas, clonadas o adulteradas, la suplantación de identidad electrónica, o cualquier otro medio fraudulento vinculado a tecnologías de la información, realizare transferencias, realizare adquisiciones de bienes o servicios, sustrajere bienes, valores o fondos económicos de cuentas bancarias, billeteras digitales o sistemas electrónicos de pago. Cuando se emplearen elementos técnicos que dificulten la trazabilidad o identificación del autor, la pena podrá elevarse hasta doce (12) años."

Artículo 10°. Reforma a la Ley 25.246. Incorpórese como artículo 20 bis de la Ley 25.246 el siguiente texto:

"Artículo 20 bis: Los sujetos obligados, deberán implementar protocolos internos para la detección temprana de ciber fraudes, en coordinación con el Registro Nacional de Incidentes de Ciber fraude, la Unidad de Información Financiera y con las autoridades judiciales competentes."

CAPÍTULO VI – DISPOSICIONES FINALES

Artículo 11°. Plazo de adaptación tecnológica. Las obligaciones previstas en los artículos 3° y 4° de la presente ley deberán ser cumplimentadas en un plazo máximo de doce (12) meses a partir de su entrada en vigencia.

La autoridad de aplicación podrá establecer un cronograma escalonado según el tipo de sujeto obligado, volumen de operaciones y grado de riesgo de fraude, pudiendo fijar plazos más breves para entidades financieras y empresas proveedoras de alcance masivo.

Artículo 13°. Reglamentación. El Poder Ejecutivo Nacional deberá reglamentar la presente ley dentro de los noventa (90) días de su publicación.

Artículo 14°. Vigencia. La presente ley entrará en vigencia a los ciento veinte (120) días de su publicación en el Boletín Oficial.

OSCAR AGOST CARREÑO

Diputado Nacional

FUNDAMENTOS

Señor Presidente:

La presente ley tiene por finalidad actualizar el ordenamiento jurídico argentino frente a una de las amenazas más crecientes y sofisticadas del siglo XXI: el fraude digital o ciber fraude.

La expansión de los medios de pago electrónicos, las billeteras virtuales, el comercio digital y los servicios financieros online ha generado nuevas oportunidades, pero también nuevos riesgos que la legislación vigente no contempla adecuadamente. Nuestro Código Penal sigue aplicando en muchos casos la figura del hurto, cuando en realidad la conducta reviste una modalidad de robo digital, mediado por engaño, suplantación o elusión de barreras de seguridad.

Este proyecto incorpora como delito autónomo el fraude electrónico, con agravantes cuando medien mecanismos técnicos para vulnerar sistemas de seguridad. A su vez, se establece la obligatoriedad de implementar medidas de autenticación como el sistema 'chip & PIN', común en países como Reino Unido, Canadá y Francia, lo que reduce drásticamente los fraudes con tarjetas clonadas o robadas.

Se incorpora también un mecanismo de trazabilidad digital: toda dirección IP, log o metadato vinculado a operaciones sospechosas podrá ser requerido judicialmente, incluso cuando el autor haya intentado ocultarse tras VPN u otros mecanismos de anonimato.

Dicha intervención, amparada por orden judicial, no constituye violación al derecho a la privacidad sino una herramienta legal de investigación penal.

Asimismo, se crea el Registro Nacional de Incidentes de Ciber fraude bajo la órbita del BCRA, con obligación de reporte de las entidades financieras, fintechs y plataformas digitales, como herramienta de prevención, transparencia y coordinación interinstitucional. El Banco Central también será autoridad de aplicación, con poder sancionatorio, técnico y normativo.

Este proyecto está emparentado con otros de mi autoría (3952-D-2025 y 4561-D-2025). El fin es el mismo, poner en debate y encontrar soluciones a estos problemas que plantean los entornos digitales.

Por todo lo expuesto, y considerando experiencias exitosas de países como España, Estonia, Estados Unidos y Reino Unido, solicito a mis pares acompañen el presente proyecto para dotar al Estado argentino de herramientas eficaces y modernas en la lucha contra los delitos financieros digitales.

OSCAR AGOST CARREÑO

Diputado Nacional