

PROYECTO DE LEY

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

"Protección Integral contra la Suplantación de Identidad"

Capítulo 1: Disposiciones generales.

Artículo 1°. Objeto de la ley. El objeto de la presente es establecer de manera integral, mecanismos para la prevención, detección, control y sanción de la suplantación de identidad en el ámbito público y privado sea esta se produzca en entornos físicos o digitales.

Artículo 2°. Derecho a la información personal registrada. Toda persona tendrá derecho a consultar en forma gratuita, periódica y unificada la totalidad de bienes, servicios y productos registrados a su nombre.

Dicha consulta solo podrá ser realizada por el titular de la información o por su representante con facultades suficientes, en las condiciones que establezca la reglamentación.

Capítulo 2. Sistema Nacional de Verificación de Identidad

Artículo 3°. Creación del Sistema Nacional de Verificación de Identidad (SNVI). Créase el Sistema Nacional de Verificación de Identidad (SNVI), de carácter obligatorio, interoperable y federal, cuya finalidad será proveer a los entes públicos

y privados de un mecanismo estandarizado, seguro y auditable de validación de identidad digital en tiempo real.

El Sistema se integrará con las bases de datos del Registro Nacional de las Personas, de la Agencia de Recaudación y Control Aduanero, el Banco Central de la República Argentina, el Ente Nacional de Comunicaciones y de otros organismos que establezca la reglamentación, bajo estándares de interoperabilidad definidos por la Autoridad de Aplicación.

La validación de identidad deberá contemplar al menos uno de los siguientes mecanismos:

- a) Validación biométrica facial contra el registro del RENAPER.
- b) Autenticación mediante firma digital o electrónica avanzada.
- c) Verificación de doble factor.

La autoridad de aplicación podrá definir otros mecanismos de validación los cuales deben resguardar la integridad de los datos y garantizar la celeridad en las transacciones.

El SNVI emitirá un código de uso único de validación por transacción (CUV), que servirá como respaldo legal de cada operación.

Artículo 4º. Obligación de verificación previa en altas de servicios o productos. Toda persona humana o jurídica que desee contratar un servicio o producto financiero, línea telefónica, cuenta digital o que impliquen consecuencias patrimoniales deberá ser validada previamente a través del SNVI mediante la obtención de un CUV valido

Ningún producto o servicio comprendido en la presente podrá ser adquirido sin la obtención de un CUV válido.

Artículo 5°. Registro Nacional de Actividades de Validación (RNAV). Créase el Registro Nacional de Actividades de Validación (RNAV) como componente técnico del SNVI, que almacenará de forma segura y trazable las validaciones realizadas, incluyendo necesariamente: Fecha, hora y entidad solicitante. Resultado de la validación. Tecnología utilizada. Dispositivo, IP y geolocalización en caso de corresponder.

Este registro será accesible únicamente por el titular de los datos o su representante con facultades suficientes o la Autoridad de Aplicación, salvo en casos donde medie orden judicial que permita el acceso a otros sujetos.

Artículo 6°. Registro de incidentes de identidad. Créase un registro nacional de incidentes de intentos de suplantación de identidad.

A dicho registro solo accederá al titular de los datos o su representante con facultades suficientes, salvo en casos donde medie orden o autorización judicial que disponga lo contrario.

Artículo 7°. Autoridad de Aplicación. El Poder Ejecutivo designará la Autoridad de Aplicación quedando facultado a la creación de un Ente específico a tales efectos.

Artículo 8°. Funciones de la Autoridad de Aplicación. La Autoridad de Aplicación tendrá las siguientes funciones:

- a) Dictar los protocolos técnicos y estándares para el SNVI.
- b) Coordinar con organismos públicos y privados la implementación del sistema.
- c). Fiscalizar y auditar los mecanismos de verificación.
- d) Establecer registros de proveedores homologados.
- e) Ordenar bloqueos preventivos y emitir alertas.
- f) Administrar el RNAV y el registro de incidentes.
- g) Diseñar campañas de concientización y asistencia a víctimas.

Artículo 9°. Compatibilidad y Complementariedad con la Ley de Protección de Datos Personales. Las disposiciones de la presente ley resultan compatibles y complementarias de la Ley 25.326 de Protección de los Datos Personales, sus modificatorias y normas complementarias.

En la implementación del Sistema Nacional de Verificación de Identidad (SNVI) y sus componentes, la Autoridad de Aplicación deberá observar estrictamente los principios y garantías previstos en dicha Ley, en particular deberá:

- a) Garantizar que el tratamiento de datos personales se realice con base en el principio de legalidad, finalidad específica, proporcionalidad y minimización de datos.
- b) Que el tratamiento se limite estrictamente a la verificación de identidad con fines de prevención del fraude y suplantación.

- c) Que toda validación registrada en el RNAV sea comunicada al titular de los datos, quien tendrá pleno derecho de acceso, rectificación, actualización y supresión conforme los artículos 14 y 16 de la Ley 25.326.
- d) Que el acceso al SNVI y al RNAV esté restringido al mínimo necesario.
- e) Elaborar los informes para homologar tecnologías o reglamentos vinculados al tratamiento masivo de datos.
- f) Garantizar el tratamiento de datos con máximas medidas de seguridad técnicas y organizativas.

Artículo 10. Informe inicial de impacto. La Autoridad de Aplicación, dentro de los noventa (90) días corridos desde la promulgación de la presente ley, deberá elaborar e implementar un estudio de evaluación del impacto de la implementación de la presente en la protección de datos personales.

Artículo 11. Implementación. La implementación del SNVI será gradual de acuerdo con el siguiente cronograma:

- a) En un plazo no mayor a ocho (8) meses, el SNVI deberá estar operativo para todos los organismos de la Administración Pública Nacional.
- b) En un plazo no mayor de doce (12) meses, deberán incorporarse las entidades financieras, billeteras virtuales, compañías de telecomunicaciones, prestadoras de servicios digitales y otras entidades privadas que manejen datos sensibles o instrumentos patrimoniales.

Artículo 12°. La Autoridad de Aplicación podrá dictar normas aclaratorias y complementarias e incluso adaptar estos plazos a las capacidades técnicas y presupuestarias de los organismos involucrados.

La modificación en los plazos de implementación en modo alguno podrá duplicar los establecidos en la presente.

Capítulo 3: Modificaciones al Código Penal

Artículo 13°. Incorporase al Código Penal de la Nación el artículo 139 ter, el que quedará redactado de la siguiente manera:

“Artículo 139 ter: Será reprimido con prisión de seis (6) meses a dos (2) años el que, sin consentimiento y con la intención de cometer un ilícito o causar perjuicio, suplantare, fingiere o se apodere de la identidad de una persona humana, aun por medios tecnológicos, utilizando su nombre, apellido, imagen, seudónimo, dirección de correo electrónico, teléfonos, perfiles en redes sociales o cualquier otra información identificatoria en entornos físicos o digitales.”

Artículo 14°. Incorporase al Código Penal de la Nación el artículo 139 quater, el que quedará redactado de la siguiente manera:

“Artículo 139 quater: La pena establecida en el artículo 139 ter se elevará a prisión de uno (1) a cuatro (4) años cuando:

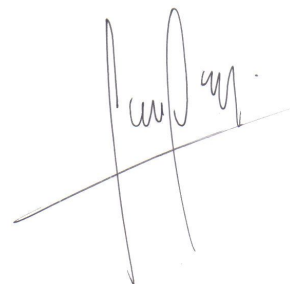
a) La víctima fuere menor de dieciocho (18) años, mayor de setenta (70) años o una persona con discapacidad;

- b) El delito se cometiere con el propósito de afectar la reputación, dignidad, intimidad o integridad sexual de la víctima;
- c) El autor actuare con el fin de obtener un beneficio económico o causar un daño patrimonial;
- d) La conducta se realizare de manera reiterada o afectare a múltiples víctimas;
- e) El autor fuere funcionario público o miembro de una fuerza de seguridad, en ejercicio de sus funciones o con abuso de su cargo."

Artículo 15°. Incorporase al Código Penal de la Nación el artículo 139 quinquies, el que quedará redactado de la siguiente manera:

"Artículo 139 quinquies: En caso de condena por el ilícito previsto en el artículo 139 ter, el juez podrá ordenar, como pena accesorio, la eliminación o rectificación del contenido digital relacionado con la suplantación, en todos aquellos espacios digitales bajo control o responsabilidad del condenado.

Artículo 16°. Comuníquese al Poder Ejecutivo.



Oscar Agust Carreño
Diputado Nacional

FUNDAMENTOS

Señor Presidente:

El objeto del presente proyecto de ley es establecer mecanismos para la prevención, detección, control y sanción de la suplantación de identidad en el ámbito público y privado sea esta se produzca en entornos físicos o digitales.

Parto del convencimiento de que el Estado debe dar una respuesta clara, concreta y urgente a una de las problemáticas más graves y extendidas de la actualidad: la suplantación de identidad.

Cada vez resultan más frecuentes los casos de suplantación de identidad lo cual acarrea numerosas consecuencias de diversa índole pudiendo incluso, generar graves perjuicios patrimoniales.

Este inconveniente tiene múltiples manifestaciones, cito como ejemplos: la creación de un perfil falso en una red social, la solicitud de un crédito, la obtención de una línea telefónica, etc. Ello la mayoría de las veces, ocurre sin que el damnificado se entere o mejor dicho, se entera cuando el daño ya está realizado.

El proyecto puede dividirse en dos partes. La Primera, apunta a la prevención, detección y control mediante la creación del Sistema Nacional de Validación de Identidad que apunta a proveer a los entes públicos y privados de un mecanismo estandarizado, seguro y auditable de validación de identidad digital en tiempo real.

La segunda parte, apunta a la sanción, introduciendo diversas modificaciones al Código Penal.

El Sistema Nacional de Validación de Identidad propuesto se integrará con las bases de datos del Registro Nacional de las Personas, de la Agencia de Recaudación y Control Aduanero, el Banco Central de la República Argentina, el Ente Nacional de Comunicaciones y de otros organismos que establezca la reglamentación, con mecanismos de validación debidamente certificados.

En modo alguno pretende retrasar o poner trabas a las transacciones. Por eso se acota a un universo específico de operaciones que podrían acarrear consecuencias patrimoniales graves como ser contratar un servicio o producto financiero, una línea telefónica, una cuenta digital o aquellos que impliquen consecuencias patrimoniales.

Asimismo, para dotar de transparencia al Sistema propuesto, como componentes del mismo, proponemos la creación de un Registro Nacional de Actividades de Validación así como otro denominado Registro de Incidentes de Identidad.

Esos registros, cabe destacar, solo serán asequibles por el titular de los datos y apuntan a la prevención, a que cualquier ciudadano pueda, en todo momento efectuar dichas consultas para controlar cualquier actividad sospechosa o que no hubiera realizado.

Esto apunta a la prevención y es similar a las herramientas que muchos entornos digitales ofrecen a fines similares, como por ejemplo, aquellos que reportan las sesiones iniciadas o incluso los intentos de inicio de sesión. Creemos que ello cambiará radicalmente la situación actual donde por lo general, cuando existe una suplantación de identidad, nos enteramos cuando se encuentra consumada y por lo general cuando ya existe un problema.

Entendemos que la autoridad de aplicación debe tener amplias facultades dentro de ciertos lineamientos que incluimos en el proyecto.

Asimismo, postulamos la compatibilidad y la complementariedad con la Ley de Protección de Datos Personales la que deberá observarse en todo momento. En cuanto a la implementación, proponemos un cronograma, pero también facultamos a la Autoridad de Aplicación a flexibilizarlo en función a las capacidades técnicas e incluso presupuestarias.

La segunda parte del proyecto, apunta a la sanción. La apropiación indebida de una identidad ajena en entornos digitales —ya sea mediante el uso del nombre, la imagen, perfiles en redes sociales, correos electrónicos o cualquier otro dato

identificadorio— es una conducta que afecta de manera directa derechos fundamentales como la identidad, la honra, la intimidad y la libertad de las personas. Esta práctica no es un “juego” ni una travesura tecnológica: es un delito que puede arruinar la vida de una persona.

Asimismo, dichas prácticas, pueden generar consecuencias, verdaderos perjuicios en la esfera patrimonial.

He recibido numerosos testimonios de víctimas cuyos perfiles fueron replicados para extorsionar, acosar o defraudar. También se han registrado casos de suplantación con fines de estafa, de violencia de género digital y hasta de acceso indebido a servicios del Estado o de instituciones privadas. Frente a esto, nuestra legislación penal guarda un silencio que ya no se puede justificar.

Por ello, proponemos incorporar al Código Penal de la Nación el delito de suplantación de identidad digital, como figura autónoma, con agravantes específicas cuando la víctima sea especialmente vulnerable o cuando el autor actúe con fines económicos, de desprestigio o desde una posición de poder.

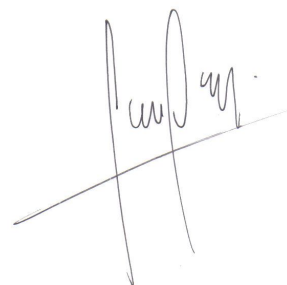
No estamos inventando nada nuevo: el mundo ya ha avanzado en este camino. España ha aprobado recientemente reformas que penalizan expresamente estas conductas, incluyendo los llamados “deepfakes”. Colombia lo hizo con la Ley 1273 desde 2009. Estados Unidos cuenta con legislación federal específica. En Argentina, en cambio, las víctimas de suplantación deben peregrinar por figuras penales inadecuadas o insuficientes.

Esta iniciativa se enmarca en una línea de trabajo que vengo sosteniendo desde hace tiempo, y que también se expresa en otros proyectos como la 'Ley Turing', destinada a regular el uso de inteligencia artificial y proteger la imagen personal. En todos los casos, el objetivo es el mismo: garantizar derechos en la era digital, construir ciudadanía tecnológica y actualizar nuestras leyes para que estén a la altura de los desafíos de nuestro tiempo.

No se trata de criminalizar el uso de la tecnología, sino de ponerle un límite claro a quienes la utilizan para dañar. La identidad de una persona no puede ser

una máscara intercambiable ni un recurso disponible para terceros. Debe ser respetada, protegida y tutelada por el Estado.

Por todo lo expuesto, solicito a mis pares que acompañen este proyecto de ley.



Oscar Agost Carreño
Diputado Nacional