DIPUTADOS
ARGENTINA

PROYECTO DE LEY

EL SENADO Y LA CÁMARA DE DIPUTADOS DE LA NACIÓN ARGENTINA
REUNIDOS EN CONGRESO SANCIONAN CON FUERZA DE LEY:

LEY DE PROTECCIÓN INTEGRAL

DE DATOS PERSONALES

(Reforma integral de la Ley Nº 25.326)

TÍTULO I – DISPOSICIONES GENERALES

ARTÍCULO 1º — *Objeto.*

La presente ley tiene por objeto la protección integral de los datos personales de las personas humanas, a fin de garantizar el ejercicio pleno de los derechos al honor, la intimidad, la autodeterminación informativa, la dignidad y la privacidad, de conformidad con lo establecido en el artículo 43, párrafo tercero, de la Constitución Nacional, los tratados internacionales de derechos humanos con jerarquía constitucional y el Convenio 108+ del Consejo de Europa. Sus disposiciones son de orden público. La presente ley deroga y reemplaza íntegramente la Ley Nº 25.326 y su Decreto Reglamentario Nº 1558/2001.

ARTÍCULO 2º — *Ámbito de aplicación.*

La presente ley se aplica al tratamiento de datos personales realizado por personas humanas o jurídicas, públicas o privadas, en todo el territorio de la República Argentina, con independencia del soporte o medio técnico utilizado.

Se aplica asimismo al tratamiento de datos personales de personas que se encuentren en territorio argentino cuando el responsable o encargado: a) se encuentre establecido en el territorio nacional; b) no se encuentre establecido en el territorio nacional pero las

actividades de tratamiento estén relacionadas con la oferta de bienes o servicios dirigidos a dichas personas, o con el monitoreo de su comportamiento en tanto éste tenga lugar en territorio argentino.

No serán de aplicación al tratamiento: a) realizado por una persona humana en actividades exclusivamente personales o domésticas; b) efectuado con fines de defensa nacional, conforme legislación específica, sin afectar el núcleo esencial de los derechos consagrados en esta ley; c) realizado en ejercicio de la libertad de expresión, prensa e información, con los límites constitucionales. En ningún caso se podrán afectar las bases de datos ni las fuentes de información periodísticas.

ARTÍCULO 3º — *Definiciones.*

A los efectos de la presente ley se entiende por:

a) Dato personal: Toda información referida a una persona humana determinada o determinable. Se considerará determinable toda persona que pueda ser identificada, directa o indirectamente, mediante un identificador como el nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, mental, económica, cultural o social.

b) Datos sensibles: Datos personales que revelen origen racial o étnico, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona, datos relativos a la salud, vida sexual u orientación sexual, neurodatos, y antecedentes penales o contravencionales.

c) Datos biométricos: Datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona que permitan o confirmen su identificación única, tales como imágenes faciales, datos dactiláricos, patrones de iris, reconocimiento de voz, patrones de marcha y neurodatos identificatorios.

d) Datos genéticos: Datos personales relativos a las características genéticas heredadas o adquiridas de una persona que proporcionen información única sobre su fisiología o salud.

e) Neurodatos: Información generada por el registro, medición o procesamiento tecnológico de la actividad del sistema nervioso central o periférico de una persona, conforme la legislación especial sobre neuroderechos. Los neurodatos se consideran datos sensibles a todos los efectos.

f) Tratamiento: Toda operación realizada sobre datos personales, automatizada o no: recolección, registro, organización, estructuración, conservación, adaptación,

modificación, extracción, consulta, utilización, comunicación, cotejo, interconexón, limitación, supresión o destrucción.

g) Responsable del tratamiento: Persona humana o jurídica, pública o privada, que determine los fines y medios del tratamiento.

h) Encargado del tratamiento: Persona humana o jurídica que trate datos por cuenta del responsable.

i) Titular de los datos: Persona humana a quien se refieren los datos.

j) Consentimiento: Manifestación de voluntad libre, específica, informada e inequívoca por la cual el titular acepta el tratamiento.

k) Elaboración de perfiles: Tratamiento automatizado consistente en utilizar datos personales para evaluar aspectos personales, en particular para analizar o predecir rendimiento profesional, situación económica, salud, preferencias, intereses, fiabilidad, comportamiento, ubicación o movimientos.

l) Seudonimización: Tratamiento de datos de manera tal que ya no puedan atribuirse a un titular sin recurrir a información adicional mantenida por separado con medidas técnicas y organizativas.

m) Anonimización: Proceso irreversible que imposibilita la identificación directa o indirecta del titular por cualquier medio razonablemente utilizable.

n) Delegado de protección de datos: Persona designada por el responsable o encargado para supervisar el cumplimiento de la normativa.

o) Violación de seguridad: Incidente que ocasione destrucción, pérdida, alteración, comunicación o acceso no autorizados a datos personales.

p) Decisión automatizada: Decisión adoptada exclusivamente sobre la base de tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos o afecte significativamente al titular.

q) Tratamiento algorítmico de alto impacto: Todo tratamiento de datos personales mediante sistemas de inteligencia artificial o algoritmos que, por su naturaleza, alcance, contexto o fines, presente un riesgo elevado para derechos fundamentales, incluyendo: decisiones sobre acceso a empleo, crédito, educación, salud, vivienda o servicios públicos esenciales; scoring o calificación social; vigilancia biométrica; y procesamiento de neurodatos con fines inferenciales.

r) Soberanía de datos: Principio según el cual los datos personales generados en territorio argentino o relativos a personas que se encuentren en la República Argentina se encuentran sujetos a la jurisdicción nacional, debiendo el Estado garantizar condiciones de independencia tecnológica en su almacenamiento, procesamiento y transferencia.

TÍTULO II – PRINCIPIOS

ARTÍCULO 4º — *Principios del tratamiento.*

El tratamiento observará los siguientes principios:

a) Licitud, lealtad y transparencia: tratamiento lícito, leal y transparente en relación con el titular.

b) Limitación de la finalidad: datos recogidos con fines determinados, explícitos y legítimos, no tratados ulteriormente de manera incompatible.

c) Minimización: datos adecuados, pertinentes y limitados a lo necesario.

d) Exactitud: datos exactos y actualizados; supresión o rectificación sin dilación de los inexactos.

e) Limitación del plazo: conservación no más tiempo del necesario para los fines del tratamiento.

f) Integridad y confidencialidad: seguridad adecuada contra tratamiento no autorizado, pérdida, destrucción o daño accidental.

g) Responsabilidad proactiva y demostrada: el responsable será responsable del cumplimiento y capaz de demostrarlo.

h) Soberanía de datos: el tratamiento respetará el principio de soberanía de datos conforme el artículo 3º inciso r) y las disposiciones del Título VII de la presente ley.

ARTÍCULO 5º — *Privacidad por diseño y por defecto.*

El responsable aplicará, tanto al determinar los medios de tratamiento como durante el tratamiento mismo, medidas técnicas y organizativas apropiadas para aplicar efectivamente los principios de protección de datos e integrar las garantías necesarias.

El responsable garantizará que, por defecto, solo sean objeto de tratamiento los datos necesarios para cada fin específico. Esta obligación se aplicará a la cantidad de datos, la extensión del tratamiento, el plazo de conservación y la accesibilidad.

TÍTULO III – BASES LEGALES DEL TRATAMIENTO

ARTÍCULO 6º — *Licitud del tratamiento.*

El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

a) El titular dio su consentimiento para uno o varios fines específicos.

b) Necesario para la ejecución de un contrato o medidas precontractuales.

c) Necesario para el cumplimiento de una obligación legal.

d) Necesario para proteger intereses vitales del titular o de otra persona.

e) Necesario para el cumplimiento de una misión de interés público o el ejercicio de potestades públicas.

f) Necesario para la satisfacción de intereses legítimos del responsable o un tercero, siempre que no prevalezcan los derechos del titular. No aplicable al tratamiento por autoridades públicas en ejercicio de sus funciones.

ARTÍCULO 7º — *Condiciones del consentimiento.*

Cuando el tratamiento se base en el consentimiento, el responsable deberá poder demostrarlo. El consentimiento será libre, específico, informado e inequívoco, prestado mediante declaración o acción afirmativa clara. El silencio, casillas premarcadas o la inacción no constituyen consentimiento.

El titular podrá retirar su consentimiento en cualquier momento, sin afectar la licitud del tratamiento previo. Retirar el consentimiento será tan fácil como darlo.

Al evaluar la libertad del consentimiento, se considerará si la ejecución de un contrato se supedita al consentimiento para tratamiento innecesario para dicho contrato.

ARTÍCULO 8º — *Tratamiento de datos sensibles.*

Queda prohibido el tratamiento de datos sensibles salvo: a) consentimiento explícito; b) cumplimiento de obligaciones laborales y de seguridad social; c) protección de intereses vitales cuando el titular no pueda consentir; d) datos manifiestamente públicos; e) formulación, ejercicio o defensa de reclamaciones; f) interés público esencial proporcional; g) fines de medicina preventiva, diagnóstico, asistencia sanitaria; h) archivo en interés público, investigación científica o estadística con garantías adecuadas.

Los neurodatos, datos biométricos y datos genéticos se considerarán datos sensibles en todas las circunstancias y requerirán las garantías reforzadas de esta ley y la legislación especial.

ARTÍCULO 9º — *Datos de niños, niñas y adolescentes.*

El tratamiento de datos de menores de dieciséis (16) años solo será lícito con

consentimiento o autorización del titular de la responsabilidad parental, conforme el principio de autonomía progresiva.

El responsable hará esfuerzos razonables para verificar dicha autorización.

Queda prohibido el tratamiento de datos de menores con fines de perfilamiento comercial, publicidad comportamental o elaboración de perfiles psicológicos o emocionales.

Los datos recopilados durante la minoría de edad deberán eliminarse a solicitud del titular al alcanzar la mayoría de edad, salvo otra base legal.

TÍTULO IV – DERECHOS DEL TITULAR

ARTÍCULO 10º — *Derecho de información.*

El responsable proporcionará al titular, al momento de la recolección, de forma clara, accesible y comprensible: a) identidad y datos de contacto del responsable y del delegado; b) fines del tratamiento y base legal; c) destinatarios o categorías de destinatarios; d) intención de transferencia internacional; e) plazo de conservación o criterios; f) existencia de derechos de acceso, rectificación, supresión, limitación, portabilidad y oposición; g) derecho a retirar el consentimiento; h) derecho a reclamar ante la Autoridad de Protección de Datos; i) existencia de decisiones automatizadas, incluida la lógica aplicada, importancia y consecuencias previstas.

ARTÍCULO 11º — *Derecho de acceso.*

El titular obtendrá del responsable confirmación de si se tratan datos que le conciernan y, en tal caso, acceso a los datos y la información del artículo anterior. El responsable facilitará copia en formato electrónico de uso común. Ejercicio gratuito, salvo solicitudes manifiestamente infundadas o excesivas.

ARTÍCULO 12º — *Derecho de rectificación.*

El titular obtendrá sin dilación la rectificación de datos inexactos y la integración de datos incompletos.

ARTÍCULO 13º — *Derecho de supresión.*

El titular obtendrá la supresión cuando: a) datos innecesarios; b) retiro del

consentimiento sin otra base legal; c) oposición; d) tratamiento ilícito; e) obligación legal.

Cuando el responsable haya hecho públicos los datos, adoptará medidas razonables para informar a otros responsables.

No procederá cuando el tratamiento sea necesario para: libertad de expresión; obligación legal; interés público en salud; archivo, investigación o estadística; formulación, ejercicio o defensa de reclamaciones.

ARTÍCULO 14º — *Derecho a la limitación del tratamiento.*

El titular obtendrá la limitación cuando: a) impugne la exactitud, durante la verificación; b) tratamiento ilícito y se oponga a la supresión; c) el responsable ya no necesite los datos pero el titular los requiera para reclamaciones; d) se haya opuesto mientras se verifica la prevalencia de motivos legítimos.

ARTÍCULO 15º — *Derecho a la portabilidad.*

El titular recibirá sus datos en formato estructurado, de uso común y lectura mecánica, y podrá transmitirlos a otro responsable, cuando el tratamiento esté basado en consentimiento o contrato y se efectúe por medios automatizados. La Autoridad de Protección de Datos establecerá los estándares de interoperabilidad.

ARTÍCULO 16º — *Derecho de oposición.*

El titular se opondrá en cualquier momento por motivos de su situación particular. El responsable cesará el tratamiento salvo motivos legítimos imperiosos prevalecientes. Respecto de mercadotecnia directa, la oposición será absoluta e incondicionada.

ARTÍCULO 17º — *Decisiones individuales automatizadas y elaboración de perfiles.*

Todo titular tiene derecho a no ser objeto de una decisión basada únicamente en tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos o le afecte significativamente.

No se aplicará cuando la decisión: a) sea necesaria para un contrato; b) esté autorizada por ley; c) se base en consentimiento explícito. En los supuestos a) y c), el responsable garantizará intervención humana, derecho a expresar el punto de vista e impugnar la decisión.

Las decisiones automatizadas no podrán basarse en datos sensibles salvo consentimiento explícito o interés público esencial con garantías adecuadas.

ARTÍCULO 18º — *Ejercicio de derechos.*

Ejercicio gratuito. Respuesta en quince (15) días hábiles, prorrogables por quince (15) más con aviso motivado. Cuando las solicitudes sean manifiestamente infundadas o excesivas, el responsable podrá cobrar tasa razonable o negarse, debiendo demostrarlo.

TÍTULO V – OBLIGACIONES DEL RESPONSABLE Y DEL ENCARGADO

ARTÍCULO 19º — *Obligaciones del responsable.*

El responsable: a) implementará medidas técnicas y organizativas apropiadas para garantizar y demostrar conformidad; b) llevará registro de actividades de tratamiento; c) cooperará con la Autoridad; d) aplicará privacidad por diseño y por defecto.

La obligación de registro no se aplicará a responsables con menos de cincuenta (50) personas, salvo tratamiento riesgoso, no ocasional, o de datos sensibles.

ARTÍCULO 20º — *Encargado del tratamiento.*

El encargado tratará datos únicamente conforme instrucciones documentadas del responsable, garantizará confidencialidad, implementará medidas de seguridad, asistirá al responsable y, al finalizar la relación, suprimirá o devolverá los datos. La relación se regirá por contrato que establezca objeto, duración, naturaleza, tipos de datos, categorías de titulares y obligaciones del responsable.

ARTÍCULO 21º — *Delegado de protección de datos.*

Designarán delegado: a) órganos del sector público; b) responsables cuyas actividades principales requieran observación habitual y sistemática a gran escala; c) responsables que traten datos sensibles a gran escala; d) entidades financieras, aseguradoras, prestadoras de salud y telecomunicaciones; e) responsables que realicen tratamientos algorítmicos de alto impacto.

El delegado gozará de autonomía funcional, no recibirá instrucciones, no podrá ser destituido ni sancionado por sus funciones y reportará al máximo nivel jerárquico.

ARTÍCULO 22º — *Evaluación de impacto.*

Antes de tratamientos de alto riesgo, el responsable realizará evaluación de impacto relativo a protección de datos.

Obligatoria al menos para: a) evaluación sistemática basada en tratamiento automatizado con efectos jurídicos; b) tratamiento a gran escala de datos sensibles, biométricos, genéticos o neurodatos; c) observación sistemática de zona de acceso público; d) uso de neurotecnologías; e) tratamiento de datos de menores a gran escala; f) tratamientos algorítmicos de alto impacto conforme artículo 3º inciso q).

Contendrá: descripción del tratamiento y fines; evaluación de necesidad y proporcionalidad; evaluación de riesgos; medidas de mitigación. Cuando la evaluación indique alto riesgo residual, el responsable consultará previamente a la Autoridad de Protección de Datos.

ARTÍCULO 23º — *Seguridad del tratamiento.*

El responsable y encargado implementarán medidas apropiadas al nivel de riesgo: seudonimización y cifrado; confidencialidad, integridad, disponibilidad y resiliencia; capacidad de restauración rápida; verificación y evaluación periódica de eficacia. La Autoridad establecerá estándares mínimos según categorías de datos y niveles de riesgo.

ARTÍCULO 24º — *Notificación de violaciones de seguridad.*

El responsable notificará a la Autoridad de Protección de Datos sin dilación y dentro de las setenta y dos (72) horas: descripción; categorías y número de afectados; contacto del delegado; consecuencias probables; medidas adoptadas.

Cuando la violación entrañe alto riesgo para derechos y libertades, comunicará al titular en lenguaje claro y sencillo.

TÍTULO VI – TRATAMIENTOS ALGORÍTMICOS DE ALTO IMPACTO E INTELIGENCIA ARTIFICIAL

ARTÍCULO 25º — *Clasificación de tratamientos algorítmicos.*

A los efectos de la presente ley, los tratamientos de datos personales mediante sistemas de inteligencia artificial o algoritmos se clasifican en los siguientes niveles. La aplicación de las obligaciones de cada nivel observará los principios de proporcionalidad y

gradualidad, considerando el estado del arte tecnológico, la dimensión del responsable, el volumen de datos tratados y el impacto efectivo sobre los derechos de los titulares. La ANPDP dictará guías orientativas sectoriales que faciliten el cumplimiento escalonado de las obligaciones del presente Título:

a) Riesgo mínimo: Tratamientos algorítmicos que no producen efectos jurídicos ni afectan significativamente a los titulares. Sujetos únicamente a las obligaciones generales de la presente ley.

b) Riesgo limitado: Tratamientos en que el titular interactúa con un sistema de IA sin que se adopten decisiones con efectos jurídicos. Sujetos a obligaciones de transparencia: el responsable informará que el titular interactúa con un sistema automatizado.

c) Alto impacto: Tratamientos algorítmicos de alto impacto conforme la definición del artículo 3º inciso q). Sujetos a las obligaciones reforzadas del presente Título.

d) Prohibidos: Tratamientos algorítmicos que: utilicen técnicas subliminales o manipuladoras para distorsionar materialmente la conducta; implementen scoring o calificación social de carácter general por autoridades públicas; empleen identificación biométrica remota en tiempo real en espacios públicos, salvo autorización judicial fundada para fines de seguridad ante amenaza inminente específica; infieran emociones en entornos laborales o educativos salvo fines médicos.

La Autoridad de Protección de Datos actualizará la clasificación mediante resolución fundada, previa consulta pública, con periodicidad bienal.

ARTÍCULO 26º — *Obligaciones reforzadas para tratamientos de alto impacto.*

Los responsables de tratamientos algorítmicos de alto impacto deberán, además de las obligaciones generales:

a) Realizar la evaluación de impacto prevista en el artículo 22 con carácter previo a la implementación y actualizarla ante cambios significativos.

b) Implementar un sistema de gestión de riesgos que identifique, evalúe, mitigue y monitoree continuamente los riesgos para los derechos del titular.

c) Garantizar la calidad de los datos de entrenamiento, validación y prueba, incluyendo la identificación y mitigación de sesgos estadísticos, históricos o de representación.

d) Asegurar la explicabilidad: el titular tendrá derecho a obtener una explicación comprensible de la lógica, la importancia y las consecuencias previstas de cualquier decisión o recomendación significativa derivada del tratamiento. El nivel de detalle de la explicación será proporcional a la gravedad de los efectos sobre el titular, pudiendo

la ANPDP establecer estándares diferenciados de explicabilidad según el sector de actividad y la complejidad técnica del sistema, sin que en ningún caso se pueda invocar el secreto comercial o industrial para denegar la explicación al titular afectado.

e) Garantizar la supervisión humana efectiva: designar personas con competencia, autoridad y acceso para supervisar el funcionamiento del sistema, interpretar sus resultados, decidir no utilizarlo o revertir sus decisiones.

f) Mantener registros de funcionamiento (logs) durante un período mínimo de tres (3) años o el que establezca la reglamentación según el sector y nivel de riesgo, que no podrá ser inferior a un (1) año ni superior a cinco (5) años. Los registros se conservarán en condiciones que garanticen su integridad y disponibilidad.

g) Someter el sistema a auditoría algorítmica independiente con periodicidad bienal, cuyos resultados serán comunicados a la Autoridad de Protección de Datos. La ANPDP podrá exigir periodicidad anual para sistemas que afecten derechos fundamentales de manera directa o que hayan presentado incidentes previos. Durante los primeros tres (3) años de vigencia de la presente ley, la primera auditoría podrá ser reemplazada por una autoevaluación documentada conforme las guías que dicte la ANPDP, salvo para tratamientos que involucren datos sensibles, neurodatos, datos biométricos o datos genéticos.

h) Publicar un resumen accesible del funcionamiento del sistema, sus fines, los tipos de datos utilizados y las medidas de mitigación de riesgos y sesgos adoptadas.

ARTÍCULO 27º — *Auditoría algorítmica.*

La auditoría algorítmica prevista en el artículo anterior evaluará como mínimo: a) el cumplimiento de los principios de la presente ley; b) la precisión, robustez y ausencia de sesgos discriminatorios del sistema; c) la eficacia de las medidas de supervisión humana; d) la adecuación de los mecanismos de explicabilidad.

Las auditorías serán realizadas por auditores independientes certificados por la Autoridad de Protección de Datos. La auditoría no requerirá acceso al código fuente completo, limitándose a la arquitectura funcional, los datos de entrenamiento, los resultados y los efectos sistémicos.

La Autoridad de Protección de Datos podrá ordenar auditorías extraordinarias cuando existan indicios fundados de vulneración de derechos.

TÍTULO VII – TRANSFERENCIAS INTERNACIONALES Y SOBERANÍA DE DATOS

ARTÍCULO 28º — *Principio general.*

Toda transferencia de datos personales a un país u organización internacional solo se realizará cumpliendo las condiciones del presente Título, a fin de asegurar que el nivel de protección garantizado por esta ley no se menoscabe.

ARTÍCULO 29º — *Transferencias basadas en decisión de adecuación.*

La Autoridad de Protección de Datos podrá declarar, mediante resolución fundada, que un país, territorio, sector o organización internacional garantiza nivel adecuado de protección. Se considerarán: el Estado de Derecho y legislación; la existencia de autoridades de protección independientes; los compromisos internacionales. Las decisiones serán revisadas cada cuatro (4) años.

ARTÍCULO 30º — *Transferencias mediante garantías adecuadas.*

A falta de decisión de adecuación, el responsable podrá transferir datos solo con garantías adecuadas y derechos exigibles: a) normas corporativas vinculantes; b) cláusulas tipo adoptadas por la Autoridad; c) cláusulas contractuales autorizadas; d) códigos de conducta aprobados con compromisos vinculantes; e) mecanismos de certificación con compromisos vinculantes.

ARTÍCULO 31º — *Soberanía de datos y localización estratégica.*

Los datos sensibles, neurodatos, datos biométricos y datos genéticos de personas que se encuentren en territorio argentino deberán contar con al menos una copia de respaldo almacenada en servidores ubicados en la República Argentina o en países con decisión de adecuación vigente.

Los datos del sector público nacional, provincial y municipal deberán almacenarse primariamente en infraestructura ubicada en territorio argentino, pudiendo utilizarse servicios de computación en la nube que cumplan con los estándares de seguridad y soberanía que establezca la Autoridad.

El Estado Nacional promoverá el desarrollo de infraestructura soberana de almacenamiento y procesamiento de datos, centros de datos nacionales y estándares de nube soberana, como condición para la independencia tecnológica en el tratamiento de datos personales.

La transferencia de datos personales a jurisdicciones que no ofrezcan garantías adecuadas podrá ser suspendida por la Autoridad de Protección de Datos mediante resolución fundada cuando existan indicios fundados de acceso masivo o sistemático

por parte de autoridades públicas del país de destino.

TÍTULO VIII – AUTORIDAD DE PROTECCIÓN DE DATOS PERSONALES

ARTÍCULO 32º — *Creación y naturaleza jurídica.*

Créase la Autoridad Nacional de Protección de Datos Personales (ANPDP) como ente autárquico con plena autonomía técnica, funcional y financiera, con personería jurídica propia, patrimonio propio y capacidad de actuación en el ámbito del derecho público y privado.

La ANPDP no recibirá instrucciones de ninguna autoridad en el ejercicio de sus funciones de control. Su presupuesto será aprobado anualmente por el Congreso de la Nación como partida específica dentro del Presupuesto General, con un piso mínimo que garantice el cumplimiento efectivo de sus funciones, el cual no podrá ser inferior al del ejercicio anterior ajustado por inflación.

ARTÍCULO 33º — *Dirección.*

La ANPDP será dirigida por un Director o Directora Nacional designado por el Poder Ejecutivo Nacional con acuerdo del Honorable Senado de la Nación, previo concurso público de antecedentes y oposición organizado por el Consejo de la Magistratura del Poder Judicial de la Nación.

El Director durará cinco (5) años en su cargo, renovable por una única vez. Deberá acreditar título universitario de abogado o equivalente, y experiencia mínima de diez (10) años en materia de protección de datos, derecho de las nuevas tecnologías o derecho constitucional.

Solo podrá ser removido mediante resolución fundada del Honorable Senado de la Nación, por las causales de mal desempeño, delito en el ejercicio de sus funciones o crímenes comunes, con mayoría de dos tercios de los miembros presentes. El procedimiento de remoción garantizará el derecho de defensa del Director.

El Director estará sujeto a las mismas incompatibilidades que los jueces federales y no podrá ejercer otra actividad profesional, comercial o de asesoramiento durante su mandato.

ARTÍCULO 34º — *Funciones.*

Son funciones de la ANPDP: a) velar por el cumplimiento de la presente ley y dictar

normas reglamentarias complementarias; b) recibir y resolver denuncias y reclamos, e iniciar actuaciones de oficio; c) realizar investigaciones, inspecciones y auditorías; d) emitir decisiones de adecuación; e) aprobar cláusulas tipo, normas corporativas vinculantes, códigos de conducta y mecanismos de certificación; f) aplicar sanciones; g) certificar auditores algorítmicos; h) publicar informe anual de actividades ante el Congreso de la Nación; i) cooperar con autoridades de protección de datos de otros países y organismos internacionales; j) promover la educación y sensibilización pública; k) establecer estándares de seguridad, interoperabilidad y soberanía de datos; l) administrar el porcentaje de multas que le corresponda conforme el artículo 37.

La ANPDP presentará un informe anual ante las Comisiones de Asuntos Constitucionales y de Comunicaciones e Informática de ambas Cámaras del Congreso, que será de acceso público.

TÍTULO IX – RÉGIMEN SANCIONATORIO Y RESPONSABILIDAD CIVIL

Capítulo 1 – Sanciones administrativas

ARTÍCULO 35º — *Infracciones y sanciones administrativas.*

Las infracciones se clasifican en:

a) Leves: Incumplimiento de obligaciones formales de registro, notificación o documentación. Sanción: apercibimiento y/o multa de hasta el cero coma cinco por ciento (0,5%) de la facturación bruta anual global del ejercicio anterior, o hasta quinientos (500) salarios mínimos vitales y móviles, lo que resulte mayor.

b) Graves: Tratamiento sin base legal; incumplimiento de derechos del titular; omisión de evaluación de impacto; incumplimiento de seguridad; transferencia no autorizada; obstrucción de la ANPDP; incumplimiento de obligaciones de auditoría algorítmica. Sanción: multa de hasta el dos por ciento (2%) de la facturación bruta anual global o hasta cinco mil (5.000) SMVM, lo que resulte mayor.

c) Muy graves: Tratamiento ilícito de datos sensibles; incumplimiento reiterado de resoluciones; ocultamiento doloso de violaciones de seguridad; tratamiento ilícito de datos de menores; uso de datos para discriminación; tratamientos algorítmicos prohibidos; violación de neurodatos. Sanción: multa de hasta el cuatro por ciento (4%) de la facturación bruta anual global o hasta veinte mil (20.000) SMVM, lo que resulte mayor.

La ANPDP podrá ordenar la cesación del tratamiento, bloqueo, supresión de datos y clausura de archivo. Graduación: naturaleza, gravedad y duración; carácter doloso o culposo; medidas de mitigación; cooperación; categorías afectadas; reincidencia; beneficio obtenido.

ARTÍCULO 36º — *Medidas cautelares.*

La ANPDP podrá adoptar medidas cautelares de bloqueo, limitación o suspensión de tratamientos cuando exista riesgo inminente para los derechos de los titulares. Las medidas serán fundadas, proporcionales y revisables judicialmente.

ARTÍCULO 37º — *Destino de las multas.*

El cincuenta por ciento (50%) de lo recaudado por multas se destinará al presupuesto operativo de la ANPDP. El cincuenta por ciento (50%) restante se destinará al Fondo de Fortalecimiento de la Protección de Datos, que financiará programas de educación

digital, investigación en privacidad y desarrollo de infraestructura soberana de datos.

Capítulo 2 – Responsabilidad civil y acciones judiciales

ARTÍCULO 38º — *Responsabilidad civil.*

Todo responsable o encargado que, por acción u omisión, provoque un daño a un titular como consecuencia de un tratamiento que infrinja la presente ley, estará obligado a indemnizarlo. El encargado solo responderá del daño causado cuando no haya cumplido las obligaciones específicamente dirigidas a él o cuando haya actuado al margen o en contra de las instrucciones del responsable.

La responsabilidad será objetiva cuando el tratamiento ilícito involucre datos sensibles, neurodatos, datos biométricos o datos genéticos, o derive de tratamientos algorítmicos de alto impacto.

El responsable solo podrá eximirse acreditando que el hecho dañoso no le es imputable en modo alguno.

ARTÍCULO 39º — *Daño automático por violación de datos.*

Toda violación de seguridad que resulte en la exposición no autorizada de datos personales generará un derecho a indemnización escalonada a favor de cada titular afectado, conforme las siguientes reglas: a) Cuando la violación involucre datos sensibles, neurodatos, datos biométricos o datos genéticos, la indemnización mínima será automática y su monto fijado anualmente por la ANPDP, sin necesidad de acreditar daño concreto. b) Cuando la violación involucre datos personales no sensibles, el titular deberá acreditar un umbral mínimo de afectación consistente en al menos uno de los siguientes supuestos: que los datos expuestos hayan sido efectivamente accedidos por terceros no autorizados; que la exposición haya generado un riesgo concreto y verificable de usurpación de identidad, fraude o discriminación; o que el responsable haya omitido la notificación oportuna prevista en el artículo 24. c) La ANPDP establecerá, mediante resolución fundada, una escala de indemnizaciones mínimas graduada según la gravedad de la violación, la categoría de datos afectados, el número de titulares involucrados y la conducta del responsable. d) No procederá la indemnización mínima automática del inciso a) cuando el responsable acredite fehacientemente que: implementó un programa integral de protección de datos conforme las mejores prácticas y estándares técnicos reconocidos internacionalmente; notificó la violación dentro del plazo del artículo 24; adoptó medidas de mitigación inmediatas y efectivas que limitaron sustancialmente el impacto de la violación; y cooperó activamente con la ANPDP y con los titulares afectados. En tal supuesto, subsistirá el derecho del titular a

reclamar la indemnización del daño efectivamente sufrido conforme las reglas generales de la responsabilidad civil. e) La ANPDP establecerá topes máximos diferenciados de indemnización mínima agregada por evento, considerando la dimensión del responsable, a fin de evitar que el régimen indemnizatorio comprometa la viabilidad económica de micro, pequeñas y medianas empresas.

Esta indemnización mínima no excluirá el derecho del titular a reclamar una indemnización superior acreditando daños adicionales. El responsable podrá solicitar la reducción de la indemnización mínima acreditando que implementó todas las medidas técnicas y organizativas razonables conforme el estado del arte y que actuó con la debida diligencia en la detección y notificación de la violación.

ARTÍCULO 40º — *Daños punitivos.*

Cuando la infracción a la presente ley fuere cometida con dolo, culpa grave o manifiesta indiferencia hacia los derechos de los titulares, el juez podrá aplicar una multa civil a favor del titular de hasta cinco (5) veces el monto de la indemnización fijada, a título de sanción pecuniaria disuasiva conforme los principios de los artículos 1714 y 1715 del Código Civil y Comercial de la Nación y la legislación de defensa del consumidor vigente. La graduación considerará la gravedad del hecho, el beneficio obtenido por el infractor, la posición de mercado del responsable, la reincidencia y el efecto disuasorio.

ARTÍCULO 41º — *Acción de protección de datos personales (hábeas data).*

La acción de protección de datos procederá para: a) tomar conocimiento de los datos almacenados y su finalidad; b) exigir rectificación, supresión, confidencialidad o actualización; c) hacer efectivo cualquier derecho del Título IV cuando el responsable no hubiere dado respuesta satisfactoria.

Competencia: juez del domicilio del titular, del responsable, o del lugar del hecho, a elección del titular. Fuero federal cuando el responsable sea organismo público nacional o los datos se interconecten en redes interjurisdiccionales.

Tramitará conforme el artículo 43 CN y normas procesales de amparo. El juez podrá disponer bloqueo provisional.

ARTÍCULO 42º — *Acciones colectivas.*

Será procedente la acción colectiva para la defensa de los derechos de esta ley cuando una pluralidad de titulares se vea afectada por un mismo tratamiento ilícito.

Legitimación activa: el Defensor del Pueblo, las asociaciones de defensa de consumidores registradas, la ANPDP y los afectados directos.

El tribunal podrá fijar honorarios de los letrados de la parte actora con base en el beneficio obtenido para la clase, como incentivo al litigio de interés público en materia de protección de datos.

TÍTULO X – RÉGIMEN DIFERENCIADO PARA MICRO, PEQUEÑAS Y MEDIANAS EMPRESAS

ARTÍCULO 43º — *Principio rector.*

El régimen diferenciado para MiPyMEs tiene por objeto simplificar las cargas administrativas y documentales del cumplimiento de la presente ley sin reducir en ningún caso los derechos de los titulares de datos personales ni las garantías esenciales de protección. La simplificación operará únicamente sobre obligaciones formales, procedimentales y documentales, nunca sobre derechos sustantivos.

ARTÍCULO 44º — *Ámbito y condiciones.*

Podrán acogerse al régimen diferenciado las micro, pequeñas y medianas empresas conforme la clasificación vigente de la autoridad competente, siempre que no traten: a) datos sensibles, biométricos, genéticos o neurodatos a gran escala; b) datos de menores a gran escala; c) tratamientos algorítmicos de alto impacto.

Las MiPyMEs que realicen dichos tratamientos quedarán sujetas al régimen general sin excepción.

ARTÍCULO 45º — *Simplificaciones.*

La ANPDP establecerá mediante resolución fundada, con intervención de las cámaras empresariales representativas, las siguientes simplificaciones:

a) Modelos simplificados de registro de actividades de tratamiento.

b) Guías prácticas de cumplimiento de evaluación de impacto.

c) Posibilidad de designar delegado de protección de datos compartido entre varias MiPyMEs.

d) Plazos de adecuación diferenciados.

e) Programas de asistencia técnica gratuita.

TÍTULO XI – DISPOSICIONES COMPLEMENTARIAS Y TRANSITORIAS

ARTÍCULO 46º — *Códigos de conducta y certificación.*

La ANPDP promoverá la elaboración de códigos de conducta sectoriales y mecanismos de certificación. Los códigos aprobados podrán servir como elemento para demostrar cumplimiento.

ARTÍCULO 47º — *Coordinación normativa.*

La presente ley se aplicará complementaria y coordinadamente con la legislación especial en materia de neuroderechos, soberanía cognitiva, inteligencia artificial, historia clínica electrónica, defensa del consumidor y toda normativa sectorial que involucre datos personales. En caso de conflicto, prevalecerá la norma que otorgue mayor protección.

ARTÍCULO 48º — *Transición de la Autoridad.*

La Agencia de Acceso a la Información Pública transferirá a la ANPDP la totalidad de sus funciones, personal, archivos y presupuesto relativos a la protección de datos personales dentro de los ciento ochenta (180) días de la entrada en vigencia de la presente ley. La Agencia de Acceso a la Información Pública subsistirá en el ejercicio de las competencias relativas al derecho de acceso a la información pública conforme la Ley Nº 27.275 y demás normativa aplicable. Hasta tanto se complete la transición, la Agencia de Acceso a la Información Pública continuará ejerciendo las funciones de Autoridad de Aplicación en materia de protección de datos personales.

ARTÍCULO 49º — *Plazo de adecuación.*

Los responsables y encargados dispondrán de veinticuatro (24) meses desde la entrada en vigencia para adecuarse al régimen general de la presente ley. Para las obligaciones del Título VI relativas a tratamientos algorítmicos de alto impacto, el plazo de adecuación será de treinta y seis (36) meses. La ANPDP establecerá un cronograma de implementación progresiva con al menos tres etapas, priorizando durante el primer año la asistencia técnica, la capacitación y la orientación por sobre las sanciones, salvo incumplimientos graves o dolosos. Las micro, pequeñas y medianas empresas que se acojan al régimen diferenciado del Título X dispondrán de un plazo adicional de doce (12) meses para el cumplimiento de las obligaciones formales y documentales.

ARTÍCULO 50º — *Derogaciones.*

Derógase la Ley Nº 25.326, el Decreto Nº 1558/2001 y toda norma que se oponga a la presente. Las referencias a la Ley 25.326 en otras leyes se entenderán hechas a la presente.

ARTÍCULO 51º — *Reglamentación.*

El Poder Ejecutivo Nacional reglamentará la presente ley dentro de los ciento ochenta (180) días de su publicación en el Boletín Oficial.

ARTÍCULO 52º — *Vigencia.*

La presente ley entrará en vigencia a los noventa (90) días de su publicación en el Boletín Oficial.

ARTÍCULO 53º — *Presupuesto.*

Los gastos que demande la implementación se atenderán con las partidas que anualmente asigne el Presupuesto General. El Poder Ejecutivo Nacional deberá incluir las partidas necesarias para la constitución y funcionamiento de la ANPDP en el proyecto de Presupuesto correspondiente al ejercicio fiscal siguiente a la sanción de la presente ley.

ARTÍCULO 54º — *Cláusula pro-innovación.*

La interpretación y aplicación de la presente ley deberá favorecer la innovación tecnológica compatible con los derechos fundamentales. Cuando existan múltiples interpretaciones razonables de una obligación establecida en esta ley, se preferirá aquella que, sin menoscabar la protección de los titulares, permita el desarrollo de nuevos productos, servicios y modelos de negocio basados en el tratamiento responsable de datos personales. La regulación no deberá imponer cargas desproporcionadas que desincentiven la investigación científica, el emprendimiento tecnológico o la competitividad de la economía digital argentina. La ANPDP evitará la duplicación de obligaciones documentales y procedimentales cuando el responsable acredite el cumplimiento de estándares internacionales equivalentes reconocidos por la Autoridad, tales como ISO/IEC 27701, ISO/IEC 42001 o los que la reglamentación

determine. Asimismo, la ANPDP publicará, dentro de los doce (12) meses de su constitución, una evaluación de impacto regulatorio del presente régimen sobre el ecosistema emprendedor y tecnológico nacional, y la actualizará bienalmente.

ARTÍCULO 55º — *Sandbox regulatorio de datos e inteligencia artificial.*

La ANPDP podrá establecer, mediante resolución fundada, un régimen de sandbox regulatorio que permita a responsables del tratamiento desarrollar y probar productos, servicios o modelos innovadores basados en datos personales o inteligencia artificial bajo condiciones controladas y supervisadas, con las siguientes características: a) Duración limitada de hasta veinticuatro (24) meses, prorrogable por una única vez. b) Participación voluntaria, previa solicitud del responsable y aprobación de la ANPDP. c) Flexibilización de obligaciones formales y documentales específicas, sin afectar en ningún caso los derechos fundamentales de los titulares ni las prohibiciones del artículo 25 inciso d). d) Supervisión continua de la ANPDP con acceso a información sobre el funcionamiento del proyecto. e) Consentimiento informado reforzado de los titulares participantes, con derecho de retiro inmediato. f) Obligación de la ANPDP de publicar los resultados y aprendizajes del sandbox para contribuir a la mejora regulatoria. La ANPDP establecerá un máximo de veinte (20) proyectos simultáneos de sandbox y priorizará aquellos con potencial de impacto positivo en salud, educación, inclusión financiera o investigación científica.

ARTÍCULO 56º — *Sello Argentina Data Trust.*

Créase el Sello Argentina Data Trust como certificación voluntaria de excelencia en protección de datos personales. La ANPDP administrará el programa de certificación, que evaluará el cumplimiento integral de la presente ley y estándares internacionales complementarios. El sello tendrá validez de tres (3) años y será renovable. Los responsables certificados gozarán de: a) presunción de cumplimiento de la presente ley, que operará como atenuante en procedimientos sancionatorios; b) reconocimiento preferente en contrataciones del sector público que involucren tratamiento de datos personales; c) facilitación de transferencias internacionales. La ANPDP promoverá el reconocimiento recíproco del sello por autoridades de protección de datos de otros países, en el marco de convenios de cooperación internacional.

ARTÍCULO 57º — *Comunicación.*

Comuníquese al Poder Ejecutivo Nacional.

LIC. MARCELA MARINA PAGANO
DIPUTADA DE LA NACIÓN

DIPUTADOS
ARGENTINA

FUNDAMENTOS

Señor Presidente:

El presente proyecto propone la reforma integral de la Ley Nº 25.326 de Protección de Datos Personales, sancionada hace más de veinticinco años en un contexto tecnológico, económico y social radicalmente diferente al actual.

I. Urgencia estratégica. La Ley 25.326 fue pionera en América Latina y permitió que la Argentina obtuviera en 2003 la declaración de nivel adecuado de protección de la Comisión Europea, un activo estratégico para la inserción de nuestro país en la economía digital global. En enero de 2024, la Comisión confirmó la adecuación pero recomendó expresamente que se consolide en legislación las protecciones desarrolladas a nivel sublegal. La próxima revisión, prevista para 2028, evaluará la conformidad sustancial con el RGPD. Sin reforma, la adecuación está en riesgo.

II. Obsolescencia normativa. La ley vigente no contempla: portabilidad de datos, privacidad por diseño, responsabilidad proactiva, decisiones automatizadas, evaluaciones de impacto, notificación de brechas, delegado de protección de datos, neurodatos, datos biométricos, transferencias con garantías adecuadas, ni interés legítimo como base legal. El anteproyecto de la AAIP perdió estado parlamentario en 2024 y los proyectos Carro/Doñate de 2025 no abordan la coordinación con la legislación emergente sobre neuroderechos, soberanía cognitiva e inteligencia artificial.

III. Cinco innovaciones críticas que distinguen este proyecto.

Primera: Autoridad independiente con blindaje institucional (Título VIII). La ANPDP se crea como ente autárquico con autonomía técnica, funcional y financiera, presupuesto propio aprobado por el Congreso con piso inflacionario, Director designado con acuerdo del Senado previo concurso público, mandato de cinco años, remoción solo por resolución fundada del Senado con mayoría calificada, e informe anual ante el Congreso. Este diseño responde a la exigencia de la Comisión Europea de independencia efectiva como condición de la adecuación, y al estándar del artículo 52 del RGPD. La Argentina había recibido críticas por la dependencia de la anterior Dirección Nacional del Poder Ejecutivo.

Segunda: Capítulo integral de IA y tratamientos algorítmicos (Título VI). El proyecto no se limita a datos: incorpora la regulación de tratamientos algorítmicos de alto impacto, alineada con la lógica del AI Act europeo (Reglamento 2024/1689). Clasifica los tratamientos en cuatro niveles de riesgo, prohibe prácticas como el scoring social y la manipulación subliminal, exige explicabilidad, supervisión humana efectiva, auditorías algorítmicas independientes anuales, y gestión de calidad de datos de entrenamiento.

Esto posiciona a la ley como instrumento “future-proof” que integra datos + IA, superando el paradigma RGPD 2016.

Tercera: Enforcement real mediante sistema de daños y litigio (Título IX, Capítulo 2). Se introducen tres mecanismos: daño automático por violación de datos (indemnización mínima fija sin necesidad de acreditar perjuicio concreto); daños punitivos de hasta cinco veces la indemnización para infracciones dolosas o gravemente culposas; y acciones colectivas con incentivos económicos para los letrados. Estos mecanismos activan el cumplimiento real de la ley, superando el problema endémico de las leyes argentinas: normas robustas con enforcement débil.

Cuarta: Soberanía de datos integrada (Título VII). Se incorpora el concepto de soberanía de datos como principio rector, exigiendo copia de respaldo en territorio argentino o países adecuados para datos sensibles, neurodatos, biométricos y genéticos; localización primaria de datos del sector público; promoción de infraestructura soberana; y facultad de la ANPDP de suspender transferencias ante indicios de acceso masivo. El diseño del Título VII ha sido calibrado para resultar compatible con las obligaciones asumidas por la República Argentina en el marco de la Organización Mundial del Comercio y el Acuerdo General sobre el Comercio de Servicios (GATS), en tanto las exigencias de localización se limitan a una copia de respaldo —no a la exclusividad de almacenamiento— y se justifican en la excepción de orden público y protección de la privacidad del artículo XIV del GATS. Esto da coherencia sistemática con el marco conceptual de soberanía cognitiva que este Congreso impulsa.

Quinta: Régimen MiPyME preciso y no debilitador (Título X). Se establece un principio rector explícito: la simplificación opera solo sobre obligaciones formales, procedimentales y documentales, nunca sobre derechos sustantivos. Las MiPyMEs que traten datos sensibles, de menores o realicen tratamientos algorítmicos de alto impacto quedan excluidas del régimen diferenciado. Esto protege contra la percepción de “puerta trasera” y es coherente con la tendencia europea de simplificación sin reducción de protección.

IV. Coordinación normativa. Este proyecto opera como ley base del ecosistema legislativo de protección de la persona en el entorno digital, articulando explícitamente con la Ley Nacional de Neuroderechos (LNDN), la Ley de Soberanía Cognitiva y Protección de la Atención Humana, y la legislación sobre inteligencia artificial soberana. Sin esta ley actualizada, esas normas sectoriales carecen del sustento operativo imprescindible.

V. Equilibrio innovación-protección. El proyecto incorpora tres mecanismos que evitan que la regulación desincentive la innovación: una cláusula pro-innovación que orienta la interpretación de la ley hacia la compatibilidad con el desarrollo tecnológico; un sandbox regulatorio supervisado por la ANPDP que permite probar productos y servicios

innovadores bajo condiciones controladas, siguiendo el modelo de Reino Unido y Singapur; y el Sello Argentina Data Trust como certificación voluntaria de excelencia exportable internacionalmente, que genera incentivos de mercado para el cumplimiento y posiciona al país como hub de confianza digital.

VI. Posicionamiento geopolitico. Con la sanción de esta ley, la Argentina se posicionará como el primer país de América Latina con un marco integrado datos + IA + neuroderechos + soberanía cognitiva, superando el modelo chileno (solo neuroderechos constitucionales), el brasileño (solo protección de datos) y el europeo (fragmentado entre RGPD y AI Act). Esta convergencia normativa fortalece la posición argentina en foros multilaterales y preserva la declaración de adecuación europea como activo estratégico.

Por todo lo expuesto, solicito a mis pares la aprobación del presente proyecto de ley.

LIC. MARCELA MARINA PAGANO
DIPUTADA DE LA NACIÓN