PROYECTO DE LEY

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

MODIFICACIÓN DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES

TÍTULO I — DISPOSICIONES GENERALES

ARTÍCULO 1° — Objeto y finalidad: La presente ley tiene por objeto establecer un marco regulatorio para la protección de los datos personales y la privacidad de las personas humanas, promoviendo el uso responsable de la información en entornos digitales, la innovación tecnológica, el desarrollo económico y la mejora de servicios. Se reconocen como fines esenciales la protección de la dignidad humana, la autonomía personal y los derechos fundamentales, en armonía con el desarrollo de tecnologías emergentes.

Esta ley parte del principio de que la información personal es una manifestación de la identidad individual y que su protección debe lograrse mediante un equilibrio entre los derechos de las personas y el desarrollo de soluciones tecnológicas que generen valor social y económico.

ARTÍCULO 2 ° — Ámbito de aplicación: Las disposiciones de esta ley se aplican a:

a) Toda persona física o jurídica, pública o privada, que trate datos personales en el territorio argentino o que ofrezca bienes o servicios a personas humanas que se encuentren en Argentina;

b) El tratamiento de datos personales de personas físicas residentes en Argentina, independientemente del lugar donde se realice el procesamiento;

c) Quien trate los datos desde una jurisdicción extranjera pero en virtud de acuerdos internacionales, contratos o vínculos jurídicos con Argentina;

d) Toda actividad de tratamiento, automatizado o no, de datos personales e inferidos que pueda tener efectos sobre personas físicas en el país;

e) Sistemas de inteligencia artificial que procesen datos personales con fines relevantes para decisiones sobre personas físicas;

f) Procesos de inferencia de datos que generen información personalizada con impacto significativo.

ARTÍCULO 3 ° — Definiciones: A los efectos de esta ley se entiende por:

a) Datos personales: toda información vinculada a una persona física identificada o identificable, ya sea de manera directa o mediante elementos que razonablemente permitan su identificación;

b) Datos sensibles: categorías especiales de datos que requieren protección reforzada por su potencial para afectar derechos fundamentales;

c) Datos inferidos: información generada a partir del análisis de datos personales preexistentes, incluyendo perfiles, predicciones o conclusiones, con capacidad de influir en decisiones sobre el titular;

d) Datos biométricos: información relativa a características físicas o conductuales que permitan la identificación única de una persona;

e) Datos genéticos: información relativa a características hereditarias o adquiridas que revelen aspectos sobre la fisiología o salud de una persona;

f) Tratamiento: cualquier operación automatizada o manual aplicada a datos personales, tales como recolección, almacenamiento, uso, transferencia o supresión;

g) Responsable del tratamiento: persona o entidad que determina los fines y medios del tratamiento de datos;

h) Encargado del tratamiento: persona o entidad que realiza el tratamiento por cuenta del responsable;

i) Titular de los datos: persona física a la que se refieren los datos personales;

j) Consentimiento: manifestación libre, informada y verificable del titular, que autoriza el tratamiento de sus datos para fines determinados, sin condicionamientos indebidos al acceso a servicios;

k) Anonimización: proceso irreversible que impide identificar al titular de los datos de manera razonable;

l) Seudonimización: proceso por el cual los datos personales son tratados de forma tal que ya no puedan atribuirse a un titular específico sin utilizar información adicional almacenada por separado y sujeta a medidas técnicas y organizativas que garantizan su no atribución;

m) Incidente de seguridad: evento que implique pérdida, acceso no autorizado o alteración indebida de datos personales;

n) Inteligencia artificial: sistemas tecnológicos capaces de realizar funciones predictivas, clasificatorias o decisorias en base al análisis de datos, definidos por objetivos humanos;

o) Decisión automatizada: decisión adoptada sin intervención humana significativa, con efectos relevantes sobre los titulares;

p) Elaboración de perfiles: tratamiento automatizado que evalúa características o comportamientos personales para segmentación, predicción o personalización;

q) Empresa con tratamiento avanzado de datos: organización que, en atención a la naturaleza, alcance, contexto y finalidades del tratamiento, realice operaciones de tratamiento de datos a gran escala, incluya de manera principal el tratamiento de datos sensibles o emplee sistemas de inteligencia artificial o mecanismos de decisión automatizada que produzcan efectos jurídicos o impactos significativos sobre los titulares;

r) Empresa con tratamiento intermedio de datos: organización que, sin encuadrar en la categoría anterior, lleve a cabo tratamientos de datos personales de alcance relevante o recurrente en el marco de su actividad, pudiendo incluir de manera accesoria o incidental el tratamiento de datos sensibles;

s) Empresa con tratamiento básico de datos: organización que realice tratamientos de datos personales de alcance limitado, no sistemáticos o de baja complejidad, sin

involucrar habitualmente datos sensibles ni procesos de decisión automatizada con impacto significativo sobre los titulares.

t) Startup o proyecto innovador: iniciativas de base tecnológica, científica o experimental con menos de cinco años de actividad y alto componente de innovación, que podrán ser beneficiarias de esquemas regulatorios diferenciales previstos en esta ley.

ARTÍCULO 4 ° — Principios generales: El tratamiento de datos personales se regirá por los siguientes principios:

a) Licitud: el tratamiento debe basarse en causales válidas previstas en la ley;

b) Finalidad: los datos deben recolectarse y tratarse con fines legítimos, explícitos y compatibles;

c) Minimización: se recolectarán solo los datos estrictamente necesarios para cumplir la finalidad declarada;

d) Exactitud: los datos deben mantenerse actualizados y verificables según su uso previsto;

e) Conservación limitada: los datos deberán conservarse sólo por el tiempo necesario para cumplir su finalidad, con revisión periódica de su pertinencia;

f) Seguridad: el tratamiento debe incluir medidas de protección técnica y organizativa proporcionales al riesgo;

g) Responsabilidad proactiva: los responsables deben anticiparse a los riesgos y demostrar cumplimiento mediante buenas prácticas y auditorías;

h) Transparencia: el titular debe contar con información clara, accesible y útil sobre el tratamiento de sus datos;

i) Proporcionalidad: las medidas de tratamiento deben ser razonables en relación al impacto previsto sobre los titulares;

j) No discriminación: queda prohibido el uso de datos personales con fines discriminatorios directos o indirectos;

k) Interpretación pro innovación responsable: las dudas de interpretación se resolverán en favor de soluciones que garanticen derechos sin desalentar prácticas tecnológicamente viables y socialmente beneficiosas;

l) Neutralidad tecnológica: esta ley es aplicable a cualquier tecnología de tratamiento, presente o futura, sin privilegiar o excluir métodos técnicos particulares.

TÍTULO III — LICITUD DEL TRATAMIENTO

ARTÍCULO 5 ° — Bases de licitud: El tratamiento de datos personales será lícito cuando se cumpla al menos una de las siguientes condiciones:

a) El titular haya otorgado su consentimiento válido;

b) Sea necesario para la ejecución de un contrato con el titular;

c) Sea requerido para el cumplimiento de una obligación legal del responsable;

d) Sea necesario para proteger intereses vitales del titular u otra persona;

e) Sea necesario para el cumplimiento de funciones de interés público expresamente reconocidas;

f) Sea necesario para satisfacer intereses legítimos del responsable o de un tercero, siempre que no prevalezcan los derechos del titular, considerando la expectativa razonable del mismo, la naturaleza del tratamiento y el impacto efectivo. Este supuesto podrá aplicarse especialmente en el contexto de innovación, desarrollo de nuevos productos, mejora de servicios o prevención de fraude, cuando se garantice un nivel adecuado de transparencia y resguardo de derechos.

ARTÍCULO 6 ° — Entrenamiento de sistemas de inteligencia artificial con datos públicos: El tratamiento de datos personales públicos para entrenamiento, desarrollo y evaluación de sistemas de inteligencia artificial será válido como interés legítimo conforme al artículo 5, inciso f), cuando:

A. Los datos sean accesibles públicamente sin restricción técnica o legal;
B. No incluyan categorías especiales de datos sensibles, salvo consentimiento explícito o fines de investigación científica y medicina preventiva;
C. El responsable implemente medidas de seguridad proporcionales al impacto y conforme a estándares internacionales;
D. El titular cuente con un mecanismo claro, gratuito y accesible para oponerse al uso de sus datos en sistemas de IA. La oposición ejercida producirá efectos a partir del siguiente ciclo de entrenamiento o actualización del modelo, debiendo el responsable documentar y acreditar ante la autoridad de aplicación la efectiva exclusión de los datos objetados;

ARTÍCULO 7 ° — Consentimiento: El consentimiento será una de las bases legales válidas para el tratamiento de datos personales, y será considerado válido cuando cumpla las siguientes condiciones:

a) Libre: otorgado sin coacción ni condicionamientos indebidos

b) Específico: referido a uno o más fines determinados o categorías claramente identificables;

c) Informado: basado en información comprensible, accesible y proporcional al uso previsto;

d) Inequívoco: manifestado mediante una acción afirmativa clara;

e) Verificable: el responsable debe poder demostrar razonablemente que lo obtuvo;

f) Revocable: el titular podrá retirarlo sin expresión de causa y con mecanismos sencillos, proporcionales y accesibles. La revocación no afectará los tratamientos realizados con anterioridad bajo base lícita.

g) Cuando se trate de menores de trece (13) años, el consentimiento deberá ser otorgado o autorizado por sus representantes legales, según parámetros adecuados a su comprensión y resguardo del interés superior del niño.

h) El consentimiento no será exigible cuando exista otra base jurídica válida, en especial en casos de:

1) Tratamientos de bajo impacto, claramente informados al titular;

2) Actividades de personalización de servicios, desarrollo interno o mejora continua;

3) Transferencias internas dentro de un mismo grupo económico, siempre que no impliquen perjuicios significativos para el titular y se respeten los principios de transparencia, minimización y seguridad;

4) Procesamiento necesario para análisis estadísticos, estudios de uso, o elaboración de modelos que no impliquen decisiones individuales automatizadas sin supervisión humana significativa.

ARTÍCULO 8 ° — Tratamiento de datos sensibles: El tratamiento de datos sensibles estará permitido cuando se configure alguno de los siguientes supuestos:

a) El titular haya prestado su consentimiento explícito;

b) Sea necesario para proteger intereses vitales del titular;

c) Se refiera a datos que el titular haya hecho públicos;

d) Sea necesario para el ejercicio o la defensa de derechos en procesos judiciales;

e) Se realice por razones de interés público;

f) Tenga por finalidad la medicina preventiva, el diagnóstico o la asistencia sanitaria;

g) Tenga fines de investigación científica o estadística.

ARTÍCULO 9 ° — Tratamiento de datos inferidos: El tratamiento de datos inferidos será válido siempre que derive de datos recolectados lícitamente y no cause efectos jurídicos o impactos significativos sobre el titular, salvo que medie revisión humana en tales casos.

La autoridad de aplicación establecerá criterios sectoriales para los tratamientos que puedan implicar un impacto elevado para la persona.

ARTÍCULO 10 ° — Supresión de datos en sistemas de inteligencia artificial ya entrenados : Cuando el titular solicite la supresión de datos personales utilizados en entrenamientos previos de sistemas de inteligencia artificial, el responsable deberá evaluar en primer término si dicha supresión es técnicamente viable sin comprometer la integridad fundamental del modelo, entendida como su estabilidad, rendimiento o funcionalidad esencial.

Si la supresión no resultara técnicamente viable, el responsable deberá documentar la imposibilidad mediante un informe técnico con carácter de declaración jurada, realizada bajo condiciones de confidencialidad frente a terceros, pero accesible para la autoridad de aplicación y para el propio titular.

En tales casos, el responsable aplicará medidas alternativas que permitan mitigar el impacto del tratamiento previo, incluyendo: el bloqueo inmediato del uso futuro de esos datos; su exclusión en nuevos ciclos de entrenamiento, ajuste o versiones posteriores del modelo; y la anonimización del registro cuando ello sea técnicamente posible.

Todo el procedimiento deberá desarrollarse con transparencia y el titular tendrá derecho a recibir una copia accesible de la fundamentación técnica correspondiente. En caso de

controversia, la autoridad de aplicación podrá ordenar una auditoría técnica independiente bajo confidencialidad.

ARTÍCULO 11 ° — Régimen de datos seudoanonimizados: Los datos personales seudoanonimizados podrán ser tratados sin el consentimiento del titular y con menor intensidad de controles cuando el tratamiento se realice con fines de:

a) Elaboración de estadísticas de interés público o sectorial;

b) Investigación científica o académica;

c) Preservación de registros históricos o de archivo de interés público;

d) Desarrollo, entrenamiento o mejora de sistemas de inteligencia artificial, conforme a los requisitos del artículo 6°.

Para que el tratamiento quede alcanzado por este artículo, deberán cumplirse las siguientes condiciones:

1) La información adicional que permita la reidentificación debe almacenarse por separado del conjunto de datos tratado, con medidas técnicas y organizativas que impidan su atribución a una persona física identificada o identificable sin acceso a dicha información adicional;

2) El responsable no utilizará los datos seudoanonimizados con el fin de reidentificar a los titulares ni permitirá su uso por terceros con ese propósito;

3) Deberá existir un protocolo documentado que describa las medidas de separación, acceso restringido y destrucción de las claves de reidentificación al concluir el tratamiento;

4) Los resultados publicados o compartidos externamente no deberán permitir la identificación individual razonable.

El régimen de datos seudoanonimizados no excluye la aplicación de los principios generales del artículo 4° ni las obligaciones de seguridad del artículo 23°. La autoridad de aplicación dictará guías sectoriales sobre estándares técnicos mínimos.

TÍTULO IV — DERECHOS DEL TITULAR

ARTÍCULO 12 ° — Derecho a la información: El titular tiene derecho a acceder, en forma clara y comprensible, a información sobre:

a) Los fines del tratamiento;

b) Las bases legales que lo justifican;

c) Sus derechos y medios para ejercerlos;

d) La identidad y datos de contacto del responsable;

e) Las transferencias realizadas o previstas.

La información podrá ser proporcionada mediante medios digitales estandarizados, formatos accesibles o interfaces automatizadas, siempre que cumplan criterios de claridad y disponibilidad razonable.

ARTÍCULO 13 ° — Derecho de acceso: El titular tiene derecho a obtener confirmación sobre si se están tratando datos personales que le conciernen, y en su caso acceder a:

a) Los datos objeto de tratamiento;

b) Las finalidades y bases legales;

c) Las categorías de datos;

d) Los destinatarios o transferencias previstas;

e) El origen de los datos si no fueron recabados directamente;

La respuesta podrá ser facilitada por medios automatizados seguros, siempre que permita la verificación de identidad y trazabilidad.

ARTÍCULO 14 ° — Derecho de rectificación: El titular podrá solicitar la corrección de datos inexactos o la actualización de datos desactualizados. Las organizaciones deberán adoptar procesos razonables para verificar la solicitud sin exigir pruebas desproporcionadas.

ARTÍCULO 15 ° — Derecho de supresión: El titular podrá solicitar la supresión de sus datos personales cuando:

a) Ya no sean necesarios para los fines para los que fueron recolectados;

b) Se haya retirado el consentimiento y no exista otra base jurídica válida;

c) El tratamiento sea manifiestamente ilegal;

d) Los datos se refieran a menores de edad recolectados sin las garantías adecuadas.

Este derecho no será exigible cuando el tratamiento resulte necesario y proporcionado para el cumplimiento de una obligación legal, la defensa de derechos en sede judicial o administrativa, o el interés público en materia de salud, seguridad o investigación científica sujeta a salvaguardas.

En caso de conflicto, la autoridad de aplicación ponderará el ejercicio del derecho frente a los intereses legítimos involucrados, conforme a principios de razonabilidad y proporcionalidad. Para el caso de datos utilizados en sistemas de inteligencia artificial, se estará a lo dispuesto en el artículo 10°.

ARTÍCULO 16 ° — Derecho a la limitación del tratamiento: El titular podrá solicitar la limitación temporal del tratamiento en los siguientes casos:

a) Impugnación de la exactitud de los datos;

b) Tratamiento ilícito y oposición a la supresión;

c) Necesidad de conservación para el ejercicio de derechos;

d) Cuando se haya ejercido el derecho de oposición.

La limitación podrá consistir en la simple suspensión del acceso interno, sin obligación de eliminación física o desindexación automática.

ARTÍCULO 17 ° — Derecho a la portabilidad: El titular podrá solicitar la entrega de sus datos en un formato estructurado, de uso común y lectura automatizada, y la transmisión directa a otro responsable cuando sea técnicamente posible y no afecte derechos de terceros.

Este derecho será aplicable a los datos proporcionados directamente por el titular y, cuando técnicamente sea viable, a los resultados de perfil o datos inferidos de alto impacto que el responsable utilice para adoptar decisiones significativas sobre el titular. No incluirá los parámetros internos de modelos, ponderaciones algorítmicas ni información técnica protegida por secreto industrial.

ARTÍCULO 18 ° — Derecho de oposición: El titular podrá oponerse al tratamiento de sus datos personales, o una finalidad específica de este, si no ha prestado consentimiento. El Responsable de tratamiento debe dejar de tratar los datos personales objeto de oposición.

No se admitirá oposición cuando el tratamiento sea necesario para fines legítimos imperiosos, tales como seguridad de la información, prevención del fraude, o mejora del sistema, salvo prueba en contrario.

ARTÍCULO 19 ° — Derecho a revisión en decisiones automatizadas: El titular tendrá derecho a solicitar la revisión de decisiones basadas exclusivamente en tratamientos automatizados que produzcan efectos jurídicos o impactos relevantes sobre sus derechos u obligaciones, así como a requerir información general sobre dichas decisiones.

El responsable deberá considerar la solicitud del titular y adoptar medidas razonables en función de la naturaleza del tratamiento, el contexto y los posibles efectos sobre el titular, pudiendo incluir la revisión con intervención humana o la adopción de medidas alternativas adecuadas.

Este derecho no será aplicable cuando la decisión automatizada resulte necesaria para la ejecución de una relación contractual, esté autorizada por normativa aplicable, o no produzca efectos jurídicos ni impactos relevantes sobre el titular. Asimismo, podrá limitarse cuando su ejercicio implique una afectación desproporcionada al funcionamiento del servicio o a intereses legítimos del responsable, siempre que se adopten salvaguardas adecuadas

TÍTULO V — OBLIGACIONES DEL RESPONSABLE

ARTÍCULO 20 ° — Obligaciones según categoría de empresa: Los responsables del tratamiento deberán cumplir con obligaciones proporcionales a la naturaleza, alcance, contexto y finalidades del tratamiento, de conformidad con la categoría de empresa en la que se encuentren encuadrados según lo dispuesto en el artículo 3°.

Empresas con tratamiento básico de datos: Deberán implementar medidas técnicas y organizativas apropiadas para garantizar la seguridad de los datos personales, mantener información de contacto accesible del responsable y atender las solicitudes de los titulares dentro de plazos razonables, pudiendo llevar registros simplificados de sus actividades de tratamiento.

Empresas con tratamiento intermedio de datos: Deberán, además de lo previsto para las empresas con tratamiento básico, implementar medidas de seguridad acordes al nivel de operación, mantener registros adecuados de sus actividades de tratamiento, adoptar políticas de privacidad claras y accesibles, y promover la capacitación del personal involucrado en el tratamiento de datos personales.

Empresas con tratamiento avanzado de datos: Deberán cumplir con las obligaciones previstas para las empresas con tratamiento intermedio y, adicionalmente, adoptar mecanismos reforzados de gestión y control del tratamiento de datos personales, incluyendo, cuando corresponda, la designación de un Delegado de Protección de Datos, la realización de evaluaciones o revisiones periódicas de sus sistemas de tratamiento, y la implementación de programas de capacitación continua del personal.

ARTÍCULO 21 ° — Principio de responsabilidad proactiva: Los responsables y encargados deberán adoptar medidas razonables, proporcionadas al riesgo, para garantizar el cumplimiento de esta ley. Estas medidas podrán incluir políticas internas, evaluación de impacto en casos de alto riesgo, capacitación y mecanismos de autorregulación. En caso de duda interpretativa, deberá privilegiarse la solución que resguarde el equilibrio entre la protección efectiva de los derechos de las personas y la promoción de la innovación responsable.

ARTÍCULO 22 ° — Registro de actividades: Los responsables y encargados mantendrán un registro actualizado de las actividades de tratamiento, en formato simplificado y accesible, cuando el volumen o el riesgo del tratamiento lo justifique. Quedan exceptuadas de esta obligación las micro y pequeñas empresas clasificadas como de tratamiento básico conforme al artículo 3°, salvo que realicen tratamiento intensivo o de datos sensibles.

ARTÍCULO 23 ° — Evaluación de impacto: Solo será exigible una evaluación de impacto previa en tratamientos que, por su naturaleza, escala o contexto, puedan implicar un riesgo elevado para los derechos de las personas. La autoridad podrá emitir guías no vinculantes para orientar criterios sectoriales.

ARTÍCULO 24 ° — Encargados del tratamiento:. Cuando un tratamiento se realice por cuenta de un tercero, el responsable deberá garantizar contractualmente que el encargado se sujete a las instrucciones y medidas adecuadas de protección de datos. El encargado podrá incorporar soluciones automatizadas, estándares de certificación o mecanismos tecnológicos para cumplir con esta obligación.

ARTÍCULO 25 ° — Notificación de incidentes de seguridad: En caso de incidentes de seguridad que puedan afectar derechos de los titulares, el responsable deberá:

a) Notificar a la autoridad de aplicación en un plazo razonable ;

b)Notificar a los titulares afectados en un plazo razonable, cuando exista probabilidad significativa de perjuicio para sus derechos, intereses o dignidad;

c) Incluir en la notificación a la autoridad: la naturaleza del incidente, las categorías y volumen aproximado de datos y titulares afectados, las posibles consecuencias del incidente, y las medidas adoptadas o previstas para mitigar sus efectos.

No se requerirá notificación pública a los titulares cuando los datos afectados estuvieran protegidos mediante cifrado u otras medidas técnicas que hagan ininteligible la información para quienes no estén autorizados a acceder a ella, de modo que el incidente no pueda producir perjuicio efectivo.

La autoridad de aplicación mantendrá un registro de incidentes notificados, de acceso público en formato agregado y anonimizado, a fin de contribuir a la evaluación de riesgos sistémicos en el ecosistema digital.

ARTÍCULO 26° — Mecanismos alternativos y autorregulación: Se promoverán mecanismos de autorregulación, certificación sectorial, programas de cumplimiento voluntario y resolución alternativa de conflictos, con reconocimiento oficial, como vía para prevenir conflictos y reducir sanciones, incluyendo estándares de cumplimiento desarrollados por asociaciones sectoriales, cámaras empresariales o consorcios tecnológicos reconocidos por la autoridad. La adopción efectiva de estos mecanismos será considerada atenuante ante la eventual imposición de sanciones.

ARTÍCULO 27 ° — Principio de cooperación público-privada: La autoridad de aplicación promoverá el diálogo técnico regular con sectores académicos, tecnológicos y empresariales para el desarrollo de orientaciones prácticas, guías sectoriales y estándares interoperables que fomenten el cumplimiento eficiente de esta ley.

TÍTULO VI — TRANSFERENCIAS INTERNACIONALES DE DATOS

ARTÍCULO 28°— Transferencias internacionales: Toda persona física o jurídica que procese datos personales en conexión con Argentina podrá hacerlo mediante transferencias internacionales bajo decisiones de adecuación, cláusulas contractuales estándar, reglas corporativas vinculantes u otros mecanismos reconocidos por la autoridad de aplicación, sin requerir almacenamiento físico de datos en Argentina como condición previa.

Cuando los datos regresen a Argentina para procesamiento, cumplimiento o servicios al titular, aplicarán todas las disposiciones de esta ley.

La autoridad de aplicación llevará un registro público de países y organizaciones con nivel de protección adecuado, actualizado al menos cada dos años. Podrá emitir órdenes de suspensión de transferencias hacia destinos que no garanticen protección equivalente, previo procedimiento contradictorio con el responsable afectado.

TÍTULO VII — LIMITACIONES Y EXCEPCIONES

ARTÍCULO 29°— Actividades periodísticas, artísticas y académicas: Esta ley no será aplicable al tratamiento de datos personales realizado en el marco de actividades periodísticas, expresivas, artísticas o académicas, en la medida en que dicho tratamiento se encuentre amparado por la libertad de expresión y no tenga como objeto principal la explotación comercial de datos. Esta exclusión se interpretará de manera amplia a favor del ejercicio de libertades fundamentales y no deberá ser utilizada para restringir ni directa ni indirectamente el derecho a informar, investigar o crear.

ARTÍCULO 30°— Acceso a la información pública: El derecho de acceso a la información pública prevalecerá sobre la protección de datos personales cuando:

a) Se refiera a funcionarios públicos en ejercicio de sus funciones;

b) Involucre el uso de recursos públicos;

c) Se relacione con políticas públicas;

d) Afecte el interés público y los datos sean pertinentes.

ARTÍCULO 31°— Fines judiciales:Los tribunales podrán ordenar el tratamiento de datos personales cuando:

a) Sea necesario para la administración de justicia;

b) Se requiera para la investigación de delitos;

c) Se necesite para el ejercicio de la defensa;

d) Se relacione con la ejecución de sentencias.

ARTÍCULO 32°— Seguridad pública: Las fuerzas de seguridad podrán tratar datos personales cuando:

a) Sea necesario para prevenir delitos;

b) Se requiera para la investigación criminal;

c) Se necesite para proteger la seguridad nacional;

d) Se relacione con la protección del orden público.

ARTÍCULO 33°— Investigación científica: El tratamiento para fines de investigación científica estará permitido cuando:

a) Sea de interés público relevante;

b) Se adopten medidas de protección apropiadas;

c) No se causen perjuicios desproporcionados al titular;

d) Los resultados no permiten la identificación individual.

ARTÍCULO 34°— Test de ponderación.: En casos de conflictos entre derechos, la autoridad de control aplicará un test de ponderación considerando los siguientes factores:

a) La naturaleza de los derechos en conflicto;

b) La intensidad de la restricción;

c) La finalidad perseguida;

d) La disponibilidad de medios alternativos;

e) El principio de proporcionalidad;

f) La situación del titular frente al responsable, considerando la asimetría de poder y recursos.

TÍTULO VIII — AUTORIDAD DE APLICACIÓN

ARTÍCULO 35°— Autoridad de aplicación: Desígnase a la Agencia de Acceso a la Información Pública (AAIP), ente autárquico creado por la Ley N° 27.275, como autoridad de contralor y aplicación de la presente ley.

El ejercicio de sus facultades se regirá por los principios de legalidad, razonabilidad y proporcionalidad, y deberá aplicarse conforme a los fines y objetivos de la presente ley, con adecuada fundamentación.

ARTÍCULO 26°— Competencias y facultades: La Agencia de Acceso a la Información Pública (AAIP) ejercerá las competencias expresamente previstas en la presente ley, las cuales deberán interpretarse de manera restrictiva, quedando excluida toda atribución implícita.

a) **Supervisión y control:** supervisar el cumplimiento de la ley mediante procedimientos reglados; investigar presuntas infracciones sobre la base de denuncia fundada o de indicios objetivos; requerir información pertinente en plazos razonables; e imponer sanciones conforme a lo previsto en esta ley, garantizando el debido proceso.

b) **Regulación:** dictar normas reglamentarias necesarias para la implementación de la ley; emitir guías de carácter no vinculante; y aprobar códigos de conducta y certificaciones de adhesión voluntaria.

c) **Promoción:** fomentar el cumplimiento mediante acciones de difusión, capacitación y asistencia técnica, priorizando mecanismos de prevención.

d) **Cooperación:** coordinar y cooperar con organismos nacionales e internacionales en el marco de sus competencias.

e) **Sanciones:** Ejercer el poder sancionatorio en base a las regulaciones establecidas en la presente ley.

f) **Registros:** Crear y administrar los registros previstos en la presente ley, conforme a los requisitos y alcances establecidos en la misma

Las actuaciones de la AAIP deberán fundarse en criterios objetivos, ser proporcionales y estarán sujetas a control judicial pleno, quedando prohibido todo ejercicio discrecional no previsto en la presente ley.

ARTÍCULO 37°— Poderes de investigación: Para el cumplimiento de sus funciones, la Agencia de Acceso a la Información Pública (AAIP) podrá:

a) Requerir información, documentación y explicaciones pertinentes al objeto de la investigación, con indicación expresa de su alcance y plazos razonables;

b) Entrevistar al personal y directivos del responsable o encargado del tratamiento, con notificación previa y posibilidad de asistencia letrada;

c) Solicitar la colaboración de otras autoridades públicas competentes;

d) Requerir dictámenes técnicos independientes y disponer la realización de peritajes cuando resulten necesarios para la determinación de los hechos, cuyo costo será soportado por la AAIP salvo que la infracción resulte acreditada;

e) Realizar auditorías de seguridad o pruebas técnicas mediante resolución fundada, con notificación previa al responsable del tratamiento y resguardo de la confidencialidad de la información;

f) Solicitar medidas cautelares a la autoridad judicial competente cuando exista riesgo inminente y grave para los derechos de los titulares de datos.

Las actuaciones deberán limitarse a los hechos bajo investigación y sustanciarse mediante procedimiento reglado que garantice el derecho de defensa, con notificación de los cargos imputados y plazo suficiente para el descargo.

ARTÍCULO 38°— Poderes correctivos y sancionatorios: En el ejercicio de sus facultades, la AAIP aplicará medidas correctivas y sanciones de manera gradual, proporcional a la gravedad de la infracción, el daño causado o potencial, la reincidencia y la cooperación del responsable durante el procedimiento. Con ese fin, podrá:

a) Emitir advertencias y recomendaciones como medida preferente ante infracciones leves o primeras infracciones sin daño concreto;

b) Ordenar el cese o la adecuación de las operaciones de tratamiento, con fijación de plazo razonable para el cumplimiento;

c) Imponer limitaciones temporales al tratamiento durante la sustanciación del procedimiento, cuando resulte necesario para prevenir riesgos, con revisión periódica.

d) Imponer limitaciones definitivas al tratamiento cuando la gravedad o reiteración de la infracción lo justifique mediante resolución fundada;

e) Ordenar la rectificación, actualización, bloqueo o supresión de datos;

f) Suspender o revocar certificaciones otorgadas, con notificación al titular de la certificación y publicidad del acto;

g) Imponer sanciones económicas conforme a lo previsto en la presente ley y de acuerdo con los criterios establecidos en el Capítulo correspondiente.

h) Emitir órdenes de suspensión de transferencias internacionales cuando el país u organización destinataria no garantice un nivel de protección adecuado conforme al Artículo 30 de la presente ley, previa evaluación documentada.

TÍTULO IX — RÉGIMEN SANCIONADOR

ARTÍCULO 39°— Infracciones:Constituyen infracciones las siguientes conductas:

Infracciones leves

a) Incumplimiento de deberes de información;
b) Deficiencias en registros y documentación;
c) Incumplimiento de términos para responder solicitudes.

Infracciones graves

a) Tratamiento sin base legal;
b) Violación de principios fundamentales;
c) Incumplimiento de derechos del titular;
d) Deficiencias en medidas de seguridad;

Infracciones muy graves

a) Tratamiento masivo de datos sensibles sin autorización;
b) Uso discriminatorio de datos inferidos;
c) Violaciones masivas de seguridad;
d) Desobediencia a órdenes de la autoridad;
e) Reincidencia en infracciones graves;
f) Obstaculización de investigaciones de la AAIP mediante ocultamiento, destrucción, falsificación o alteración de documentos, o negativa de acceso a instalaciones.

ARTÍCULO 40°— Régimen sancionatorio: La autoridad podrá imponer sanciones proporcionales a la gravedad de la infracción, al comportamiento previo del responsable, al

daño ocasionado, al volumen del tratamiento y al beneficio obtenido de la infracción. Las sanciones podrán consistir en:

a) Advertencias o requerimientos de adecuación;

b) Multas económicas calculadas según los siguientes criterios:

1. Infracciones leves: hasta el cero coma cinco por ciento (0,5%) de la facturación anual en la República Argentina del infractor;
2. Infracciones graves: hasta el dos por ciento (2%) de la facturación anual en la República Argentina del infractor por actividades vinculadas a la infracción;
3. Infracciones muy graves: hasta el tres por ciento (3%) de la facturación anual en la República Argentina del infractor por actividades vinculadas a la infracción;

c) Suspensión temporal del tratamiento en supuestos críticos;

d) Publicación de la resolución, cuando resulte disuasiva y proporcional.

Las micro y pequeñas empresas clasificadas como de tratamiento básico podrán beneficiarse de un régimen diferenciado de sanciones y plazos de adecuación, salvo en casos de reiteración o negligencia grave. Los topes aplicables en estos casos serán los del nivel leve, con independencia de la clasificación de la infracción.

TÍTULO X — DISPOSICIONES ESPECIALES

ARTÍCULO 41°— Protección de menores: El tratamiento de datos personales de personas menores de edad requerirá el consentimiento de sus representantes legales cuando se trate de menores de trece (13) años, debiendo el responsable implementar mecanismos razonables para verificar la edad del titular y la validez del consentimiento otorgado.

El responsable deberá adoptar medidas adecuadas para garantizar la protección de los datos de personas menores de edad, considerando la naturaleza del tratamiento y los riesgos asociados, y limitar su recolección y uso a lo estrictamente necesario. El incumplimiento de estas obligaciones dará lugar a la aplicación de las sanciones previstas en la presente ley.

ARTÍCULO 42°— Código de conducta:La autoridad de aplicación podrá promover la elaboración de códigos de conducta de adhesión voluntaria, orientados a establecer buenas prácticas en el tratamiento de datos personales, incluyendo criterios éticos, estándares sectoriales, mecanismos de autorregulación y esquemas de certificación.

ARTÍCULO 43°— Certificación: La autoridad de aplicación podrá establecer o reconocer mecanismos de certificación de adhesión voluntaria en materia de protección de datos personales, orientados a acreditar el cumplimiento de buenas prácticas y estándares adecuados en el tratamiento de datos.

Dichos mecanismos podrán comprender, entre otros, sistemas de gestión de datos, tecnologías de protección, procedimientos de tratamiento, formación de personal y auditorías especializadas. La autoridad podrá definir criterios generales de referencia, promover su adopción por parte de los responsables y reconocer esquemas desarrollados

por entidades públicas o privadas que cumplan condiciones de transparencia, objetividad e independencia.

ARTÍCULO 44°— Investigación e innovación: La autoridad de aplicación promoverá el desarrollo de tecnologías, herramientas y prácticas orientadas a la protección de datos personales, fomentando la investigación aplicada, la innovación y la adopción de soluciones que integren la privacidad desde el diseño.

A tal efecto, podrá impulsar entornos de prueba, lineamientos técnicos y mecanismos de colaboración con el sector público y privado, con el objeto de facilitar el desarrollo y la implementación de tecnologías de preservación de la privacidad, incluyendo técnicas de anonimización y seudonimización, sin imponer obligaciones adicionales a las previstas en la presente ley.

TÍTULO XI — ACCIÓN DE HÁBEAS DATA

ARTÍCULO 45°— Derecho al hábeas data:Toda persona tiene derecho a ejercer la acción de hábeas data para:

a) Tomar conocimiento de los datos personales que le conciernen y de su finalidad;
b) Exigir la rectificación, actualización, inclusión o supresión de sus datos;
c) Hacer cesar el tratamiento de datos cuando éste sea ilícito;

ARTÍCULO 46°— Procedimiento extrajudicial previo: Antes de iniciar la acción judicial, el interesado deberá agotar la vía administrativa mediante solicitud directa al responsable del tratamiento, quien deberá responder en un plazo máximo de quince (30) días hábiles.

La respuesta deberá ser:

a) Clara y comprensible;
b) Completa respecto a lo solicitado;
c) Gratuita para el solicitante;
d) Por escrito o medio electrónico verificable.

En caso de negativa y/o silencio del responsable, o insatisfacción con la respuesta, se podrá acudir a la Autoridad de Aplicación, que deberá responder al titular en un plazo máximo de treinta (30) días. Pasados los treinta (30) días quedará habilitada la vía judicial, aún en caso de silencio.

ARTÍCULO 47°— Legitimación activa: Podrán ejercer la acción de hábeas data:

a) El titular de los datos personales;
b) Sus representantes legales;
c) Los sucesores universales en caso de fallecimiento;
d) El defensor oficial cuando corresponda;
e) Las organizaciones de consumidores con personería jurídica;
f) El Defensor del Pueblo de la Nación;
g) Las asociaciones de consumidor y protección de datos reconocidas.

ARTÍCULO 48°— Competencia y trámite:La acción de hábeas data tramitará según las disposiciones de la presente Ley y, supletoriamente, según el procedimiento que corresponde a la acción de amparo común y según las normas procesales en lo atinente al juicio sumarísimo. El Juez dispone de amplias facultades para adaptar los procedimientos de acuerdo a las circunstancias particulares del caso y con el fin de dar mayor eficacia tuitiva al proceso.

ARTÍCULO 49°— Contenido de la demanda:La demanda deberá contener:

a) Datos personales del actor y su domicilio;

b) Identificación del responsable del tratamiento demandado;

c) Descripción clara del derecho que se pretende ejercer;

d) Hechos que motivan la acción;

e) Prueba documental del agotamiento de la vía administrativa previa;

f) Petitorio concreto;

g) Firma del interesado o de su representante.

El actor podrá actuar sin patrocinio letrado si así lo solicitara expresamente, conforme al principio de gratuidad y accesibilidad de esta acción.

ARTÍCULO 50°— Trámite abreviado: Una vez presentada la demanda:

a) El juez verificará el cumplimiento de los requisitos formales;

b) Se correrá traslado al demandado por cinco (5) días hábiles;

c) Con la contestación de demanda o vencido el plazo, se dictará sentencia;

d) Excepcionalmente, se podrá ordenar una medida de prueba si fuera indispensable;

e) No serán admisibles excepciones dilatorias que no sean de puro derecho;

f) El juez debe resolver en un plazo máximo de treinta (30) días desde la presentación de la demanda.

ARTÍCULO 51°— Medidas cautelares:El juez podrá decretar las siguientes medidas cautelares:

a) Suspensión inmediata del tratamiento cuestionado;

b) Prohibición de transferir los datos a terceros;

c) Prohibición de destruir o alterar los datos;

d) Anotación preventiva de la medida en registros públicos;

e) Cualquier otra medida que considere necesaria para proteger los derechos del titular.

Las medidas cautelares se decretarán sin necesidad de caución cuando se trate de datos sensibles.

ARTÍCULO 52°— Efectos de la sentencia: La sentencia que haga lugar a la acción podrá:

a) Ordenar el cese del tratamiento ilícito;

b) Ordenar la rectificación, actualización o supresión de datos;

c) Establecer el derecho del actor a acceder a sus datos;

d) Fijar las condiciones futuras de tratamiento;

e) Imponer costas al demandado vencido;

f) Ordenar la publicación de la sentencia cuando sea necesario para reparar el daño;

g) Establecer astreintes para el caso de incumplimiento.

ARTÍCULO 53°— Procedimiento simplificado para consultas:Para el simple acceso a información sobre datos personales, se establece un procedimiento simplificado:

a) Solicitud: mediante formulario simple disponible en línea;

b) Identificación: con documento de identidad o firma digital;

c) Respuesta: en un plazo máximo de diez (10) días hábiles;

d) Gratuidad: sin costo para el solicitante;

e) Formato: en forma clara y comprensible.

ARTÍCULO 54°— Recurso de apelación: Las resoluciones dictadas en el marco de la presente ley serán apelables. La sentencia definitiva será apelable ante la Cámara de Apelaciones correspondiente. Las medidas cautelares serán recurribles mediante recurso de reposición, con apelación en subsidio.

El recurso deberá interponerse dentro de los cinco (5) días hábiles y se concederá en relación y con efecto suspensivo, salvo respecto de las medidas cautelares. Su trámite se ajustará al procedimiento abreviado correspondiente.

ARTÍCULO 55°— Ejecución de sentencia:La sentencia firme se ejecutará de manera inmediata, sin necesidad de promover un nuevo proceso, ante el mismo juez que la dictó. El juez contará con las facultades necesarias para asegurar su efectivo cumplimiento, pudiendo imponer sanciones conminatorias progresivas en caso de incumplimiento.

El incumplimiento de la sentencia podrá dar lugar a las responsabilidades previstas en la legislación vigente por desobediencia a la autoridad judicial.

ARTÍCULO 56°— Acción colectiva:Cuando la violación de la presente ley afecte a un número plural de personas, podrá promoverse acción colectiva a fin de tutelar los derechos involucrados. Estarán legitimados para ello las organizaciones de consumidores, el Defensor del Pueblo y las asociaciones especializadas, conforme a la normativa aplicable.

El proceso se sustanciará de acuerdo con el trámite previsto para los procesos colectivos, debiendo garantizarse una adecuada publicidad del mismo, a fin de asegurar el conocimiento y la eventual participación de los sujetos alcanzados. En este marco, el juez adoptará las medidas necesarias para una gestión eficiente del proceso y la adecuada representación de los intereses en juego.

La sentencia que se dicte producirá efectos respecto de todos los sujetos comprendidos en la clase, en los términos que se establezcan en la resolución. En caso de corresponder indemnizaciones, su distribución se realizará mediante mecanismos equitativos que aseguren una adecuada reparación de los daños.

ARTÍCULO 57°— Gratuidad y accesibilidad:A fin de garantizar el acceso efectivo a la justicia en el marco de la presente ley, se asegurará la gratuidad del proceso para el actor, mediante la exención de tasas y costas en los términos que establezca la reglamentación.

Asimismo, se facilitará el acceso a patrocinio jurídico gratuito a través de defensorías oficiales u otros mecanismos previstos en la normativa aplicable, y se dispondrán herramientas que promuevan la accesibilidad del procedimiento, incluyendo formularios simples, asistencia técnica en sedes judiciales y la utilización de medios electrónicos.

El proceso podrá desarrollarse mediante plataformas digitales en todo el territorio nacional, garantizando la identificación de las partes y la trazabilidad de las actuaciones. Las audiencias podrán celebrarse de manera virtual cuando resulte posible y conveniente, conforme a las reglas que aseguren el debido proceso

ARTÍCULO 58°— Acciones judiciales:Sin perjuicio de las sanciones administrativas, el titular de datos podrá:

a) Iniciar acciones civiles por daños y perjuicios;
b) Solicitar medidas cautelares urgentes;
c) Ejercer la acción de hábeas data;
d) Iniciar acciones colectivas cuando corresponda;
e) Acceder a procedimientos judiciales expeditos.

ARTÍCULO 59°— Prescripción:Las acciones civiles prescribirán a los tres (3) años desde que el titular tuvo conocimiento del daño y de la persona responsable, y en ningún caso más de diez (10) años desde la producción del hecho dañoso.

TÍTULO XII — SANDBOX REGULATORIO

ARTÍCULO 60°— Sandbox regulatorio:La autoridad de aplicación podrá autorizar, mediante resolución fundada, la implementación de entornos regulatorios de prueba para proyectos innovadores que involucren el tratamiento de datos personales, incluyendo aquellos basados en inteligencia artificial, nuevos modelos de negocio o mecanismos alternativos de cumplimiento.

Las autorizaciones tendrán carácter temporal y podrán prever condiciones diferenciadas o excepciones limitadas respecto de las obligaciones establecidas en la presente ley, en la medida en que ello resulte necesario para el desarrollo del proyecto y no implique un riesgo significativo para los derechos de los titulares.

El régimen de sandbox deberá regirse por los principios de flexibilidad, proporcionalidad y facilitación de la innovación, evitando la imposición de requisitos o cargas regulatorias que desvirtúen su finalidad como entorno de prueba controlado.

La reglamentación establecerá lineamientos generales para su implementación, los cuales deberán limitarse a lo estrictamente necesario para garantizar la protección de los titulares y la transparencia del proceso, sin introducir condiciones que obstaculicen o restrinjan irrazonablemente el acceso o funcionamiento de los proyectos autorizados.

ARTÍCULO 61°— Tipos de sandbox y régimen temporal:Los proyectos aprobados podrán encuadrarse en distintas modalidades de sandbox, en función de su naturaleza tecnológica, nivel de riesgo y objetivos de validación, incluyendo, entre otras, aquellas

orientadas al desarrollo de tecnologías de privacidad, al análisis de supuestos de incertidumbre regulatoria o al ensayo de sistemas avanzados de inteligencia artificial.

Las autorizaciones de sandbox tendrán carácter temporal y su duración será determinada por la autoridad de aplicación en función de las características del proyecto, pudiendo ser prorrogadas mediante resolución fundada cuando ello resulte justificado.

Al finalizar o interrumpirse el período de sandbox, el responsable deberá adoptar medidas adecuadas en relación con los datos personales tratados durante el piloto, incluyendo, según corresponda, su incorporación a un régimen de tratamiento regular, su anonimización o su supresión, así como documentar los resultados obtenidos y las condiciones de funcionamiento del proyecto.

La autoridad de aplicación podrá requerir la presentación de información o reportes finales cuando resulte necesario para la evaluación del sandbox, y establecer lineamientos generales para el cierre de los proyectos, asegurando un enfoque proporcional al riesgo.

TÍTULO XIII — DISPOSICIONES FINALES

ARTÍCULO 62°— Cooperación internacional: La República Argentina promoverá la cooperación internacional en materia de protección de datos personales, a través de mecanismos bilaterales y multilaterales, el intercambio de buenas prácticas y la participación en foros y redes especializadas.

A tal efecto, podrá impulsar el desarrollo de estándares internacionales, celebrar acuerdos de reconocimiento mutuo y fomentar la armonización normativa, en particular a nivel regional, así como brindar asistencia técnica a otros Estados.

ARTÍCULO 63°— Adhesión de provincias:Se invita a las provincias y a la Ciudad Autónoma de Buenos Aires a adherir a las disposiciones de la presente ley y a coordinar con la autoridad nacional la aplicación uniforme de sus principios.

ARTÍCULO 64°— Vigencia escalonada: La presente ley entrará en vigencia de la siguiente manera:

a) Los artículos 1° a 5° (disposiciones generales y principios): a los ciento ochenta (180) días de su publicación;

b) Los artículos 12° a 29° (derechos y obligaciones generales): a los doce (12) meses de su publicación;

c) Los artículos referidos a datos inferidos: a los dieciocho (18) meses de su publicación;

d) Las disposiciones sobre inteligencia artificial: a los treinta (30) meses de su publicación;

e) El régimen sancionador completo: a los veinticuatro (24) meses de su publicación;

f) La acción de hábeas data: a los doce (12) meses de su publicación;

g) El régimen de datos seudonimizados del artículo 11°: a los dieciocho (18) meses de su publicación;

h) Las demás disposiciones: a los doce (12) meses de su publicación.

La Ley N° 25.326 y su normativa reglamentaria quedarán derogadas a los doce (12) meses de la publicación de la presente ley, plazo a partir del cual entrarán en vigencia las disposiciones enumeradas en el inciso b). Durante el período comprendido entre la publicación y la derogación de la Ley N° 25.326, ambas normas coexistirán y en caso de conflicto prevalecerá la que otorgue mayor protección al titular.

ARTÍCULO 65°— Período de transición: Durante los primeros dos años de vigencia:

a) Se otorgará un período de gracia para el cumplimiento gradual;

b) La autoridad priorizará la asistencia técnica sobre las sanciones;

c) Se implementarán programas de apoyo para la adaptación;

d) Se desarrollarán herramientas de autodiagnóstico;

e) Se establecerán incentivos para el cumplimiento temprano.

ARTÍCULO 66°— Evaluación y revisión: La autoridad de aplicación realizará una evaluación integral de la ley cada cinco (5) años, considerando:

a) La eficacia de las disposiciones;

b) La evolución de las amenazas a la privacidad;

c) Las mejores prácticas internacionales;

d) Las necesidades de actualización normativa;

e) El balance entre protección e innovación.

ARTÍCULO 67°— Abrogación y derogación.

a) Derógase la Ley N° 25.326 de Protección de Datos Personales y su normativa reglamentaria, conforme al calendario previsto en el artículo 73°.

b) Deróganse todas las disposiciones de igual o menor jerarquía que se opongan a la presente ley.

ARTÍCULO 68°— Reglamentación: El Poder Ejecutivo Nacional reglamentará la presente ley dentro del plazo de ciento ochenta (180) días desde su publicación en el Boletín Oficial, debiendo considerar especialmente:

a) Los procedimientos específicos para el ejercicio de derechos;

b) Los criterios técnicos de seguridad y protección;

c) Los requisitos para la certificación de sistemas y para la acreditación de Delegados de Protección de Datos;

d) Los protocolos de transferencia internacional;

e) Los mecanismos de coordinación institucional;

f) Los procedimientos de investigación y sanción;

g) Los formularios y procedimientos para la acción de hábeas data;

h) Los estándares técnicos mínimos de seudoanonimización por sector de actividad;

i) Los formatos interoperables para el ejercicio del derecho de portabilidad.

ARTÍCULO 69°— Disposición transitoria especial: Los tratamientos de datos personales en curso al momento de entrada en vigencia de esta ley deberán adaptarse a sus disposiciones en los siguientes plazos:

a) Tratamientos de datos comunes: dieciocho (18) meses;

b) Tratamientos de datos sensibles: doce (12) meses;

c) Sistemas de inteligencia artificial: veinticuatro (24) meses;

d) Procesos de generación de datos inferidos: dieciocho (18) meses.

Durante este período, los responsables deberán presentar un plan de adecuación a la autoridad de aplicación.

ARTÍCULO 70°— Disposición transitoria para procedimientos en curso: Los procedimientos administrativos y judiciales iniciados bajo la vigencia de la Ley N° 25.326 continuarán su tramitación conforme a la normativa anterior, salvo que el titular de los datos solicite expresamente la aplicación de la nueva ley cuando ello le resulte más favorable.

ARTÍCULO 71°— Comunicación y difusión. La autoridad de aplicación deberá implementar un plan integral de comunicación de la nueva ley que incluya:

a) Campañas de difusión masiva en medios de comunicación;

b) Material informativo en lenguaje simple y accesible;

c) Capacitaciones gratuitas para empresas y organizaciones;

d) Guías prácticas por sector de actividad;

e) Herramientas de autodiagnóstico y cumplimiento;

f) Portal web especializado con recursos y consultas;

ARTÍCULO 72°— Comuníquese: Comuníquese al Poder Ejecutivo.

Autor: YEZA, Martín

FUNDAMENTOS

El presente proyecto propone la reforma integral del régimen de protección de datos personales vigente en la República Argentina, cuya normativa principal data del año 2000.

Se trata de un marco legal concebido en un contexto tecnológico, económico y social sustancialmente distinto del actual. En aquel momento, la circulación de datos era limitada, no existían plataformas digitales de escala global, las redes sociales no tenían la incidencia que hoy poseen y la inteligencia artificial no formaba parte de los procesos productivos ni de la vida cotidiana.

En ese contexto, los datos personales eran relevantes, pero no constituían aún un activo central en la estructura económica ni un elemento determinante en la innovación tecnológica.

La transformación ocurrida en las últimas décadas ha modificado de manera profunda el rol de los datos personales. Actualmente, su tratamiento se encuentra en la base de múltiples actividades económicas, servicios digitales y procesos de toma de decisiones, tanto en el sector privado como en el público.

Esta evolución impone la necesidad de actualizar el marco normativo, no sólo para garantizar una protección efectiva de los derechos de las personas, sino también para dotar al sistema de reglas claras, previsibles y adaptadas a las dinámicas tecnológicas contemporáneas.

En este sentido, el proyecto reafirma como eje central la protección de los datos personales como derecho fundamental, entendiendo que su resguardo efectivo constituye una condición indispensable para el funcionamiento de entornos digitales confiables y para la vigencia plena de otros derechos vinculados, tales como la privacidad, la autonomía personal y la libertad individual.

Asimismo, se reconoce que la protección de los datos personales no sólo responde a una exigencia jurídica o institucional, sino que también constituye un elemento clave para el desarrollo sostenible de los ecosistemas digitales. La existencia de reglas claras, previsibles y técnicamente adecuadas fortalece la confianza de los usuarios y permite a los actores económicos operar con mayor seguridad jurídica, internalizando la protección de datos como parte integrante de sus procesos y modelos de negocio.

En este marco, el proyecto propone instrumentar dicha protección mediante herramientas regulatorias acordes a la realidad tecnológica actual, que contemplen la complejidad de los tratamientos de datos y permitan su aplicación efectiva en contextos dinámicos. A tal fin, se adopta un enfoque basado en principios, gestión de datos y proporcionalidad, orientado a garantizar un nivel adecuado de tutela de los derechos de las personas, evitando al mismo tiempo cláusulas que puedan obstaculizar el desarrollo de la innovación y la actividad económica.

La experiencia comparada muestra que los modelos regulatorios excesivamente rígidos tienden a generar barreras innecesarias, mientras que aquellos basados en principios, gestión de impactos y proporcionalidad permiten alcanzar niveles adecuados de protección sin afectar el dinamismo de los ecosistemas digitales.

En particular, el caso de Corea del Sur resulta ilustrativo por la forma en que ha logrado combinar un estándar elevado de protección de derechos con una visión estratégica del uso

de los datos en la economía digital. A partir de reformas recientes, el sistema coreano evolucionó hacia un modelo que reconoce el valor de los datos como insumo para la innovación, sin abandonar el eje en la protección de las personas.

Este proceso implicó una revisión integral del enfoque regulatorio, orientada a dotar de mayor claridad, previsibilidad y adaptabilidad a la normativa. Corea avanzó hacia un esquema que prioriza principios, criterios objetivos y una articulación más dinámica entre regulación y desarrollo tecnológico, evitando rigideces que pudieran quedar rápidamente desactualizadas. El resultado ha sido un marco que fortalece la confianza en el uso de los datos y, al mismo tiempo, habilita su aprovechamiento en sectores estratégicos.

En paralelo, otras jurisdicciones han seguido caminos convergentes. El Reino Unido ha impulsado ajustes a su régimen con foco en la proporcionalidad y la simplificación regulatoria, buscando reducir cargas innecesarias sin afectar los niveles de protección. Por su parte, Singapur ha desarrollado un enfoque pragmático que combina reglas claras con instrumentos que acompañan la innovación, promoviendo el uso responsable de los datos en un entorno de alta competitividad tecnológica.

El proyecto se inscribe en esta línea de evolución regulatoria, procurando articular un sistema que preserve los principios esenciales de la protección de datos personales mientras que al mismo tiempo incorpore herramientas modernas que permitan su aplicación efectiva en entornos tecnológicos complejos. En este marco, se adoptan soluciones que buscan reducir la incertidumbre jurídica, limitar la discrecionalidad en la aplicación de la norma y establecer criterios objetivos para el cumplimiento por parte de los sujetos obligados.

Uno de los ejes centrales de la reforma es la incorporación de un régimen específico para el tratamiento de datos seudonimizados.

Siguiendo experiencias comparadas, en particular del derecho coreano, se reconoce que la aplicación de técnicas adecuadas de seudonimización permite reducir significativamente los riesgos para los titulares de los datos, habilitando al mismo tiempo su utilización para fines de investigación, estadística, desarrollo tecnológico e inteligencia artificial.

El proyecto establece condiciones precisas para su tratamiento, incluyendo la separación funcional de la información, la prohibición de reidentificación y la exigencia de medidas técnicas y organizativas adecuadas.

Asimismo, se introduce una regulación expresa del tratamiento de datos inferidos, contemplando la creciente relevancia de los procesos de análisis y modelización en la economía digital. El proyecto admite su tratamiento cuando deriven de datos obtenidos lícitamente y no generen efectos jurídicos ni impactos significativos sobre el titular. Esta solución busca compatibilizar la protección de las personas con el desarrollo de servicios basados en analítica de datos, inteligencia artificial y sistemas predictivos.

En relación con los datos sensibles, se mantiene un estándar reforzado de protección, en línea con los principales instrumentos internacionales, se introduce una delimitación más precisa de los supuestos habilitantes para su tratamiento. Ello permite evitar interpretaciones excesivamente amplias o restrictivas, brindando mayor seguridad jurídica a los operadores y facilitando actividades legítimas, tales como la investigación científica, la prestación de servicios de salud o el desarrollo de políticas públicas basadas en evidencia

En estos ámbitos, el uso adecuado de datos personales resulta fundamental para el avance del conocimiento, la mejora de los tratamientos, la prevención de enfermedades y el fortalecimiento de los sistemas sanitarios.

En este sentido, la norma procura no sólo resguardar los derechos de los titulares, sino también brindar a estos sectores herramientas claras y previsibles que les permitan desarrollar sus actividades sin incertidumbre regulatoria. La protección de los datos personales, correctamente instrumentada, se configura así como un elemento que no sólo protege a las personas, sino que también habilita y potencia el desarrollo de áreas críticas para el bienestar social y el progreso del país.

En materia de inteligencia artificial, el proyecto introduce una regulación específica para el entrenamiento de sistemas a partir de datos públicos, reconociendo la centralidad de estos procesos en el desarrollo tecnológico contemporáneo. La norma parte de la premisa de que los datos accesibles públicamente constituyen un insumo legítimo para la innovación, siempre que su utilización se realice bajo condiciones claras que resguarden los derechos de las personas.

A tal efecto, se establecen límites y salvaguardas orientadas a garantizar un uso responsable de la información, incluyendo la exclusión de datos sensibles y la exigencia de medidas de seguridad proporcionales al riesgo del tratamiento. Asimismo, se reconoce el derecho del titular a oponerse a la utilización de sus datos en estos procesos, incorporando mecanismos que obligan a su exclusión en ciclos futuros de entrenamiento.

Este enfoque busca compatibilizar la protección de los derechos individuales con la necesidad de no restringir de manera desproporcionada el desarrollo de tecnologías de inteligencia artificial, evitando soluciones que, bajo una lógica prohibitiva, terminen desplazando capacidades de innovación fuera del país. En cambio, se propone un esquema que establece reglas claras y operativas, permitiendo el desarrollo de estas tecnologías dentro de un marco de responsabilidad y previsibilidad.

Por otro lado, la normativa en cuestión reconoce que la economía digital opera en un entorno esencialmente transnacional, donde los flujos de datos resultan indispensables para el funcionamiento de múltiples actividades productivas, tecnológicas y de servicios. En este contexto, establecer un sistema que permita transferencias seguras y previsibles resulta fundamental para la inserción internacional del país, el desarrollo de la industria tecnológica y la atracción de inversiones.

Es por eso que el proyecto incorpora un régimen moderno y alineado con las prácticas internacionales, que constituye uno de los aspectos centrales de la reforma. Se habilita la circulación transfronteriza de datos mediante mecanismos reconocidos, evitando la imposición de requisitos de localización obligatoria que podrían generar barreras innecesarias al comercio digital y a la prestación de servicios globales.

Asimismo, el proyecto asegura la continuidad de la protección de los datos personales, estableciendo que la normativa nacional mantendrá su aplicación en los supuestos de reingreso de la información, y facultando a la autoridad de aplicación a evaluar niveles de adecuación y, en su caso, restringir transferencias hacia jurisdicciones que no garanticen estándares equivalentes de protección. De este modo, se construye un esquema que combina apertura y resguardo, permitiendo la integración al ecosistema global de datos sin resignar la tutela de los derechos de las personas.

El proyecto incorpora, además, la figura de los entornos de prueba regulados (sandbox), en línea con las tendencias regulatorias adoptadas en distintas jurisdicciones. Estos espacios permiten el desarrollo y testeo de nuevas tecnologías bajo condiciones controladas, facilitando la experimentación y la adaptación normativa en función de la evidencia. Se trata de una herramienta que busca evitar la obsolescencia regulatoria y acompañar el ritmo de la innovación tecnológica sin comprometer los estándares de protección.

En materia de cumplimiento, se establece un sistema de obligaciones diferenciadas según la categoría de los sujetos obligados, tomando en consideración el volumen de datos tratados, la complejidad de las operaciones y el nivel de usuarios involucrado. Este enfoque, alineado con los principios de proporcionalidad presentes en diversas regulaciones internacionales, permite evitar cargas desproporcionadas para pequeñas y medianas empresas, al tiempo que exige mayores niveles de responsabilidad a quienes operan con grandes volúmenes de datos o generan impactos significativos.

Es importante remarcar que la normativa establece una delimitación expresa del alcance de la ley en relación con el ejercicio de la libertad de expresión, estableciendo que el régimen de protección de datos personales no resultará aplicable a tratamientos realizados en el marco de actividades periodísticas, artísticas o académicas, siempre que no persigan un fin comercial principal. Esta previsión reconoce la necesidad de evitar interferencias indebidas sobre derechos fundamentales, garantizando que la protección de datos no se convierta en un instrumento que limite la circulación de ideas, la producción cultural o la investigación académica.

En línea con ello, se establece también la prevalencia del acceso a la información pública en aquellos supuestos en los que exista un interés público relevante. La norma busca asegurar que la protección de los datos personales no obstaculice el control ciudadano, la transparencia en el ejercicio de la función pública ni el acceso a información vinculada con el uso de recursos estatales o la adopción de políticas públicas.

Ambas disposiciones reflejan una concepción integral de los derechos fundamentales, en la que la protección de los datos personales convive y se coordina con otros derechos de igual jerarquía, evitando soluciones que, bajo una interpretación aislada, puedan generar restricciones indebidas o efectos contrarios al funcionamiento de una sociedad democrática.

Finalmente, el régimen sancionatorio adopta criterios de gradualidad y proporcionalidad, priorizando la corrección de conductas y la regularización del incumplimiento. Se establecen parámetros objetivos para la determinación de sanciones, vinculados a la gravedad de la infracción, el daño causado y la conducta del responsable, con el objetivo de garantizar previsibilidad y limitar márgenes de discrecionalidad en la actuación de la autoridad de aplicación.

En definitiva, el presente proyecto propone una actualización integral del régimen de protección de datos personales, orientada a dotar al país de una herramienta normativa acorde a los desafíos del siglo XXI. Se trata de una ley que reafirma la centralidad de los derechos de las personas en el entorno digital, pero que al mismo tiempo incorpora criterios de racionalidad, proporcionalidad y previsibilidad, indispensables para su aplicación efectiva en contextos tecnológicos complejos.

La iniciativa busca superar modelos regulatorios que han quedado desfasados frente a la realidad actual, avanzando hacia un esquema que brinde certezas tanto a los titulares de los datos como a los actores que desarrollan actividades basadas en su tratamiento. En este sentido, se promueve un marco que fortalece la confianza, reduce la incertidumbre jurídica y permite al país integrarse de manera competitiva en la economía global de los datos.

En un contexto de acelerada transformación tecnológica, contar con reglas claras, modernas y equilibradas no constituye únicamente una necesidad jurídica, sino una condición estratégica para el desarrollo. Este proyecto se inscribe en esa lógica, proponiendo una regulación que protege, ordena y habilita, sentando las bases para un ecosistema digital sólido, confiable y orientado al crecimiento sostenido.

Por todo lo expuesto, es que solicito el acompañamiento de mis pares.

Autor: YEZA, Martín