PROYECTO DE LEY

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

"DE LA CESION DE DATOS PERSONALES EN LA ORBITA ESTATAL Y DE LA EVALUACION DE IMPACTO SOBRE EL TRATAMIENTO DE DATOS PERSONALES"

ARTÍCULO 1°: SUSTITUYASE el artículo 2° de la Ley 25.326, el que queda redactado de la siguiente manera:

"*Artículo 2°:* *(Definiciones)*

A los fines de la presente ley se entiende por:

— ***Datos personales****: Información de cualquier tipo referida a persona humana o jurídica determinadas o determinables.*

— ***Datos sensibles:*** *Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.*

— ***Archivo, registro, base o banco de datos****: Indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.*

— ***Tratamiento de datos:*** *Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de*

datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

— ***Responsable de archivo, registro, base o banco de datos:*** *Persona humana o jurídica pública o privada, titular de un archivo, registro, base o banco de datos.*

— ***Datos informatizados****: Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado.*

— ***Titular de los datos:*** *Toda persona humana o jurídica con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley.*

— ***Usuario de datos:*** *Toda persona humana o jurídica pública o privada, que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos.*

— ***Disociación de datos:*** *Todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable.*

— ***Incidente de seguridad:*** *Evento que en cualquier fase del tratamiento comprometa la confidencialidad, integridad o disponibilidad de los datos personales.*

— ***Identificador único:*** *Identificador creado tecnológicamente que puede vincularse razonablemente a una persona o dispositivo. Esto incluye identificadores de dispositivos, direcciones IP, cookies, balizas web, etiquetas de píxeles, identificadores de publicidad en móviles, y tecnologías similares, números de cliente, pseudónimos únicos, alias de usuario, números de teléfono o cualquier otro tipo de identificador persistente o probabilístico que se vincule o pueda vincularse razonablemente a una persona o dispositivo determinado.*

— ***Cookies:*** *archivos creados por los sitios web, que permite almacenar información sobre los sitios que el usuario ha visitado o visita.*

— ***Dato biométrico:*** *Dato personal único, relativo a las características físicas, fisiológicas o asociadas al comportamiento, que permite o confirma la identificación única de dicha persona, como la imagen facial o datos dactiloscópicos, entre otros.*

— ***Dato genético:*** *Dato personal único relacionado a características genéticas heredadas o adquiridas de una persona natural que proporcionan información única sobre la fisiología o salud de un individuo."*

— ***Disociación de información y dato:*** procedimiento, método o técnica digital que impide vincular un dato o información con su titular.

ARTÍCULO 2°: SUSTITUYASE el artículo 5° de la Ley 25.326, el que queda redactado de la siguiente manera:

*"**Artículo 5°:** (Consentimiento).*

1. El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias.

El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el artículo 6° de la presente ley.

2. No será necesario el consentimiento cuando:

a) Los datos se obtengan de fuentes de acceso público irrestricto;

b) Se recaben exclusivamente para el ejercicio de funciones específicas de los poderes del Estado dentro del marco de sus competencias asignadas por ley o en virtud de una obligación legal clara, concreta y específica;

c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio;

d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento;

e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley 21.526.

3. La invocación de competencias legales genéricas o de finalidades institucionales amplias no constituye por sí sola base legítima suficiente para el tratamiento o la cesión de datos personales sin consentimiento del titular en los términos del inciso 2.b) del presente artículo. En todos los casos, el tratamiento o la cesión deberá ser necesario, adecuado y proporcional al fin específico que se invoque, y limitarse a los datos estrictamente indispensables para el cumplimiento de ese fin."

ARTÍCULO 3°: SUSTITUYASE el artículo 6° de la Ley 25.326, el que queda redactado de la siguiente manera:

"Artículo 6°: *(Información).*

Cuando se recaben datos personales se deberá informar previamente y de manera expresa, clara, especifica y transparente al titular de los datos sobre los siguientes aspectos:

a) La finalidad específica para la cual se tratarán los datos personales y los posibles destinatarios o cesionarios pertinentemente identificados;

b) Los tipos de datos personales que se tratarán y la base legal que justifica su tratamiento;

c) La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad, domicilio e información de contacto de su responsable;

d) El carácter obligatorio o facultativo de proporcionar los datos solicitados;

e) Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos;

f) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de sus datos personales;

g) Las medidas de seguridad, técnicas, administrativas y de cualquier otra naturaleza, implementadas para proteger los datos personales;

h) Si correspondiese, información detallada sobre el uso de cookies y tratamiento de datos mediante identificadores únicos, incluyendo el tipo y cómo los usuarios pueden gestionar los mismos;

i) Si correspondiese, las condiciones bajo las cuales los datos personales pueden ser transferidos internacionalmente, incluyendo las garantías aplicables.

El responsable del archivo o usuario de datos personales debe publicar una política de privacidad, que debe ser clara, no engañosa, comprensible para el titular de datos y fácilmente accesible. Como

mínimo, debe contener la información señalada en el presente artículo. La publicación de la política de privacidad no implica por sí sola el cumplimiento del deber de información."

ARTÍCULO 4°: SUSTITUYASE el artículo 9° de la Ley 25.326, el que queda redactado de la siguiente manera:

*"**Artículo 9°:** (Seguridad de los datos).*

1. El responsable o usuario del archivo de datos, o quien por cuenta de aquellos preste servicios de tratamiento de datos personales, debe adoptar medidas de seguridad, técnicas y administrativas que resulten idóneas y razonables para garantizar la confidencialidad, integridad y disponibilidad de los datos personales, de modo de evitar su adulteración, pérdida, acceso o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

2. Las medidas de seguridad requeridas en el párrafo precedente deben ser idóneas y razonables considerando el volumen, naturaleza, alcance, contexto y sensibilidad del tratamiento de datos personales; el tamaño del responsable o usuario del archivo de datos; y el estado de la técnica actual.

3. Cuando el responsable o usuario del archivo de datos sea una entidad perteneciente al Sector Público Nacional de conformidad con el artículo 8° de la Ley N° 24.156 o tratase datos personales de más de cien mil (100.000) personas con domicilio en el país, las medidas de seguridad referidas en el párrafo 1 del presente artículo deben incluir, como mínimo, las siguientes prácticas:

a) cifrado u otro tipo de encriptación robustas y modernas para el almacenamiento y transmisión seguras de los datos personales;

b) controles de acceso con permisos limitados a lo necesario para el cumplimiento estricto de las funciones encomendadas al personal o de terceros autorizados;

c) evaluación de riesgos periódicas que identifiquen vulnerabilidades potenciales en los sistemas, redes e infraestructuras, y concretamente, en las prácticas de tratamiento de datos personales;

d) plan de respuesta ante incidentes de seguridad que permita reaccionar rápida y eficazmente cuando datos personales resulten comprometidos; y

e) entrenamiento y capacitación continúa del personal en la seguridad y gestión de la información.

4. El responsable o usuario del archivo de datos debe notificar al órgano de control y a los titulares la ocurrencia de un incidente de seguridad que entrañe un riesgo o daño relevante a los titulares.

La referida notificación debe realizarse dentro de las setenta y dos (72) horas de que se haya tomado conocimiento del incidente. Si no fuese materialmente posible cumplir con la notificación en el plazo previsto, este podrá extenderse hasta los siete (7) días corridos, acreditando objetivamente los motivos de la dilación.

La notificación debe contener, como mínimo, la siguiente información:

a) la naturaleza o el tipo de incidente;

b) los datos personales que se estiman comprometidos;

c) el impacto potencial del incidente en los intereses de los titulares;

d) las medidas correctivas adoptadas por el responsable o usuario del archivo para abordar el incidente, incluyendo aquellas para mitigar los posibles efectos dañinos y prevenir futuros incidentes;

e) recomendaciones al titular de los datos sobre las medidas que este pueda adoptar para proteger sus intereses;

f) medios a disposición del titular para que pueda contactar al responsable o usuario del archivo de datos para mayor información.

5. Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad."

ARTÍCULO 5°: SUSTITUYASE el artículo 11 de la Ley 25.326, el que queda redactado de la siguiente manera:

*"**Artículo 11°:** (Cesión).*

1. Los datos personales objeto de tratamiento sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo.

2. El consentimiento para la cesión es revocable.

3. La cesión de datos personales que se efectúen entre entes públicos en el marco de una obligación legal, interés público o ejercicio de poderes públicos, como todo tratamiento realizado con los datos cedidos, serán lícitos en la medida que se cumplan las siguientes condiciones:

a) Esté expresamente autorizada por una ley especial, y la cesión sea necesaria para el cumplimiento de un fin público asignado por ley a la entidad receptora de los datos;

b) Que los datos cedidos sean necesarios para el cumplimiento de ese fin asignado y que la entidad receptora cuente con medidas de seguridad y protocolos necesarios para garantizar la integridad, disponibilidad y confidencialidad dispuestas en esta ley;

c) Que la entidad cedente haya obtenido los datos legalmente, de acuerdo a alguno de los supuestos previstos en el artículo 5°, y en el ejercicio de las competencias asignadas por ley;

d) La entidad receptora utilice los datos para una finalidad comprendida dentro del marco de sus competencias legales y no sea distinta de aquella con la que los datos se recolectaron originalmente;

e) Los datos sean únicamente los pertinentes y estrictamente necesarios para dar cumplimiento a la finalidad pública, de conformidad con el principio de minimización de datos.

4. En los supuestos previstos en el inciso 3 del presente artículo no será exigible el consentimiento cuando:

a) En los supuestos previstos en el artículo 5° inciso 2, con excepción del punto b, al que se le aplicarán las reglas del inciso 3 de este artículo;

b) Se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados;

c) Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos sean inidentificables.

5. El cesionario quedará sujeto a las mismas obligaciones legales y reglamentarias del cedente y éste responderá solidaria y conjuntamente por la observancia de las mismas ante el organismo de control y el titular de los datos de que se trate.

6. La transferencia de datos sensibles entre entidades públicas deberá estar motivada en una ley, cumplir con los principios de necesidad y proporcionalidad, y autorizada por el órgano de control previa evaluación de impacto sobre el derecho a los datos personales. La entidad receptora de los datos podrá utilizar los datos sensibles exclusivamente para la finalidad que le dio origen a la cesión, quedando prohibido todo uso ulterior indistintamente que sea compatible con sus funciones. Cumplido dicho objetivo, la entidad receptora deberá suprimir los datos o la autoridad cedente revocar el acceso a la base compartida. No serán aplicables estas reglas a las transferencias de datos sensibles realizadas entre entidades que cumplen las mismas funciones en distintas esferas del Estado.

7. Las empresas y sociedades del Estado como las sociedades de economía mixta recibirán el mismo tratamiento que las personas jurídicas privadas, en los términos de esta Ley. Cuando el objetivo de estas entidades consista en instrumentar o ejecutar políticas públicas, recibirán el mismo tratamiento que las personas jurídicas y organismos públicos en los términos de este artículo.

8. Las entidades y personas jurídicas públicas tienen prohibido transferir a las personas jurídicas privadas datos personales, excepto:

a) En los casos de ejecución descentralizada de actividades públicas que requieran la cesión, exclusivamente para este fin específico y particular;

b) Cuando así lo establezca una ley, la cesión sea necesaria, adecuada y proporcional al fin específico que la justifica en los términos del artículo 5° inciso 3, y esté respaldada por contratos, convenios o instrumentos análogos debidamente publicados.

En todos los supuestos, las personas jurídicas privadas cesionarias deben cumplir con la totalidad de las disposiciones de la presente ley.

9. El acceso directo, la interconexión o la interoperabilidad permanente entre bases de datos personales de entidades del Sector Público Nacional, cualquiera sea el medio técnico empleado, queda equiparado a la cesión de datos personales a los efectos de la presente ley y sujeto a las condiciones establecidas en el inciso 3 del presente artículo. En ningún caso, la interconexión entre bases de datos podrá habilitar un acceso indiscriminado o masivo a datos personales que exceda los estrictamente necesarios para el cumplimiento de la finalidad específica que la justifica."

ARTÍCULO 6°: INCORPÓRASE el artículo 12 bis a la Ley 25.326, conforme el siguiente texto:

*"**Artículo 12° bis:** (Evaluación de impacto sobre la protección de datos).*

1. Si el responsable o usuario del archivo prevé realizar algún tipo de tratamiento de datos que, por su naturaleza, alcance, contexto o finalidades, entrañe un alto riesgo de afectación a los derechos de los titulares de los datos amparados en la presente ley, deberá realizar, de manera previa a la implementación del tratamiento, una evaluación del impacto relativa a la protección de los datos personales.

2. La evaluación de impacto sobre la protección de datos será obligatoria en los siguientes casos, sin perjuicio de otros supuestos que establezca el órgano de control:

a) Cuando el tratamiento de datos implique una observación sistemática y a gran escala de datos personales sensibles, datos biométricos que tengan por objeto identificar de manera unívoca a una persona, datos genéticos, o de datos relativos a antecedentes penales o contravencionales;

b) Cuando el tratamiento implique una evaluación sistemática y exhaustiva de datos personales, basados en un tratamiento automatizado de datos, incluida la elaboración de perfiles, sobre cuya base se produzcan efectos significativos a los derechos, libertades e intereses legítimos del titular de los datos;

c) Cuando el tratamiento hecho a gran escala involucre datos personales de niñas, niños o adolescentes, o de otros grupos vulnerables;

d) Para la observación sistemática a gran escala de una zona de acceso público.

3. La evaluación de impacto debe incluir, como mínimo:

a) Una descripción detallada de las operaciones de tratamiento de datos propuestas, incluyendo la naturaleza, alcance, contexto y los propósitos del tratamiento;

b) Un análisis de la necesidad y proporcionalidad del tratamiento de datos en relación con la finalidad declarada;

c) La identificación y evaluación de los riesgos para los derechos, libertades e intereses legítimos de los titulares de datos potencialmente afectados por el tratamiento;

d) La indicación de las medidas de mitigación de los riesgos identificados, incluidas las garantías, medidas de seguridad y todo otro mecanismo que garantice la protección de los datos personales.

La evaluación de Impacto sobre la protección de datos debe ser presentado al órgano de control previo a todo proceso de recolección, almacenamiento y tratamiento de los datos personales."

ARTÍCULO 7°: INCORPÓRASE como artículo 12 ter de la Ley 25.326 con el siguiente texto:

***"Artículo 12° ter**. (Delegado de protección de datos).*

ES obligatoria la designación de un delegado de protección de datos personales, en los siguientes casos:

a) Cuando se trate de un ente perteneciente al Sector Público Nacional;

b) Cuando las actividades de tratamiento de datos efectuadas por el responsable o usuario del archivo requieran una supervisión continua por su volumen, alcance, contexto o finalidades, de conformidad con las disposiciones de la presente ley y sus normas reglamentarias.

Cuando el responsable o usuario del archivo de datos sea un ente perteneciente al Sector Público Nacional que tuviese varias dependencias subordinadas obligadas a su designación, se podrá designar un único delegado de protección de datos, teniendo en cuenta su estructura organizativa y tamaño.

El delegado de protección de datos deberá reunir los requisitos de idoneidad, capacidad, y en particular, conocimientos específicos en la materia de protección de datos, que determine el órgano de control."

ARTÍCULO 8°: INCORPÓRASE como artículo 12 quater de la Ley 25.326 con el siguiente texto:

"Artículo 12° quater: (*Funciones del delegado*).

SON funciones del delegado de protección de datos:

1) Asesorar al responsable o usuario del archivo de datos, a su personal y al encargado del tratamiento, sobre las disposiciones contenidas en esta ley, sus normas complementarias, reglamentaciones y otras regulaciones emitidas por el órgano de control;

2) Supervisar el cumplimiento de las disposiciones contenidas en esta ley, sus normas complementarias, reglamentaciones y otras regulaciones emitidas por el órgano de control;

3) Asesorar en el análisis de riesgos, evaluaciones de impacto a la protección de datos y sobre las medidas de seguridad, y supervisar su aplicación;

4) Cooperar con el órgano de control y actuar como punto de contacto con dicha entidad, en relación con las cuestiones relacionadas con el tratamiento de datos.

Las funciones del delegado de protección de datos serán ejercidas libremente, sin interferencias de ningún tipo. Para su correcto desempeño, se le deberán asignar los elementos y recursos necesarios."

ARTÍCULO 9°: INCORPÓRASE como artículo 22 bis de la Ley 25.326, conforme el siguiente texto:

*"**Artículo 22° bis**. (Registro de cesiones realizadas).*

Las entidades del Sector Público Nacional de conformidad con lo previsto por el artículo 8° de la Ley 24.156, deben llevar un registro actualizado de todas las cesiones de datos personales efectivamente realizadas, el que contiene, como mínimo, la siguiente información:

1) la identificación de la entidad cedente y de la entidad o persona cesionaria;

2) la base legal que autoriza la cesión;

3) la finalidad específica de la cesión;

4) las categorías de datos personales cedidos;

5) el volumen estimado de titulares de datos alcanzados;

6) la fecha de la cesión y, en su caso, el plazo de vigencia del acceso otorgado;

7) las medidas de seguridad adoptadas para la transferencia.

El registro previsto en el presente artículo será puesto a disposición del órgano de control y podrá ser consultado por los titulares de datos en ejercicio de su derecho de acceso.

El órgano de control podrá reglamentar las condiciones, plazos y modalidades de actualización del registro, como su publicación periódica con la debida disociación de los datos personales."

ARTÍCULO 10°: SUSTITUYASE el artículo 31 de la Ley 25.326 de Protección de los Datos Personales, el que queda redactado de la siguiente manera:

*"**Artículo 31°:** (Sanciones y medidas correctivas).*

El órgano de control podrá aplicar a los infractores de la presente ley, las siguientes sanciones:

a) apercibimiento;

b) suspensión de las actividades relacionadas con el tratamiento de datos hasta tanto se cumpla con los requisitos previstos en la presente ley.

c) multa de hasta el dos por ciento (2%) de los ingresos neto de la persona jurídica responsable o usuario del archivo de datos, grupo o conglomerado empresarial teniendo en cuenta las declaraciones impositivas correspondientes al último año fiscal;

d) Cancelación de la inscripción en el Registro establecido por la presente ley, del archivo, registro o banco de datos.

En cualquiera de los casos, el órgano de control podrá exigir que se adopten medidas correctivas. Estas incluirán, pero no se limitarán, a:

i) Revisión y modificación de los procesos de tratamiento de datos para asegurar el cumplimiento normativo y una efectiva protección;

ii) Capacitación obligatoria en protección de datos para el personal involucrado en el tratamiento de los mismos;

iii) Auditorías periódicas realizadas por terceros independientes para evaluar la conformidad de las normativas de protección de datos personales;

iv) Implementación de sistemas de gestión de calidad y seguridad de la información certificados por normas reconocidas internacionalmente.

En caso de que un ente del Sector Público Nacional cometa una infracción a la presente ley o a las que la complementen, el órgano de control podrá imponer las medidas correctivas tendientes a restaurar el cumplimiento normativo y mejorar la protección de datos, pudiendo aplicar, además, las sanciones previstas en el presente artículo, al funcionario público responsable del tratamiento de datos y al delegado de protección de datos respectivo, ello sin perjuicio de las sanciones civiles, disciplinarias y penales que le pudiere corresponder."

ARTÍCULO 11°: INCORPÓRASE como artículo 31 bis de la Ley 25.326, con el siguiente texto:

*"**Artículo 31° bis.** (Graduación).*

El órgano de control determinará la adecuación de las medidas correctivas y de las sanciones administrativas con base en los siguientes criterios:

1) la gravedad de la infracción y la dimensión del daño o peligro a los intereses legítimos de los titulares de datos;

2) la ventaja económica obtenida por el infractor o por terceros, en virtud de la comisión de la infracción;

3) la condición económica del infractor;

4) la buena fe y cooperación del infractor;

5) la reiteración o reincidencia;

6) la negativa u obstrucción a la acción investigadora o de vigilancia por el órgano de control;

7) la adopción de medidas correctivas y mecanismos y procedimientos tendientes al tratamiento seguro y adecuado de los datos personales y capaces de mitigar los daños;

8) la proporcionalidad entre la gravedad de la infracción y la sanción;

9) la notificación oportuna de incidentes de seguridad."

ARTÍCULO 12°: INCORPÓRASE como artículo 31 ter de la Ley 25.326, con el siguiente texto:

*"**Artículo 31° ter**. (Potestad del Órgano de Control).*

El órgano de control se encuentra facultado, además de las potestades que surgen de la presente ley a:

1) Determinará las condiciones y procedimientos operativos, para la constatación del cumplimiento de las disposiciones de la presente ley, sus reglamentaciones, normas complementarias;

2) Iniciar los procedimientos sancionatorios por violaciones e infracciones a la presente ley, a los siguientes:

a) a instancia del titular de los datos personales;

b) por denuncia de un tercero, asociaciones u organizaciones con un interés legítimo.

c) de oficio.

En todos los supuestos se deberá garantizar el derecho al debido proceso y los principios de publicidad y celeridad procesal. En particular, cuando la acción fuese instada por el titular de los datos personales, se deberá asegurar además la gratuidad del procedimiento.

La resolución será recurrible conforme las disposiciones de la Ley 19.549. Sin perjuicio de ello, los recursos que se interpongan contra las resoluciones dictadas en el marco de la presente ley tendrán efecto devolutivo. La interposición de recursos administrativos o acciones judiciales no suspenderá la ejecutoriedad de las sanciones aplicadas, salvo que el juez competente, a petición de parte y mediante resolución fundada, dispusiera la suspensión cautelar de la sanción impugnada. "

ARTÍCULO 13°: SUSTITUYASE el artículo 33 de la Ley 25.326, el que queda redactado de la siguiente manera:

*"**Artículo 33°.** (Procedencia).*

1. La acción de protección de los datos personales o de hábeas data procederá:

a) Para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes sobre la finalidad de aquéllos, de las medidas de seguridad, técnicas, administrativas y de cualquier otra naturaleza aplicadas a estos;

b) En los casos en que se presuma la falsedad, inexactitud, desactualización en la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido en la presente ley, para exigir su rectificación, supresión, confidencialidad o actualización."

ARTÍCULO 14°: SUSTITUYASE el artículo 34 de la Ley 25.326, el que queda redactado de la siguiente manera:

*"**Artículo 34°.** (Legitimación activa).*

La acción de protección de los datos personales o de hábeas data podrá ser ejercida por el afectado, sus tutores o curadores y los sucesores de las personas humanas, sean en línea directa o colateral hasta el segundo grado, por sí o por intermedio de apoderado.

Cuando la acción sea ejercida por personas jurídicas, deberá ser interpuesta por sus representantes legales, o apoderados que éstas designen al efecto.

En el proceso podrá intervenir en forma coadyuvante el Defensor del Pueblo y el órgano de control de esta ley, quien será notificado del inicio de la acción.

La acción de hábeas data podrá ser entablada en representación colectiva de personas humanas, por el afectado, el Defensor del Pueblo o las asociaciones u organizaciones con interés legítimo, siempre que su objeto se limite a la impugnación de tratamientos de datos personales que conlleven, violaciones legales generalizadas o afectaciones a intereses individuales homogéneos."

ARTÍCULO 15°: Adecuación de convenios vigentes

TODOS los convenios, acuerdos, protocolos o instrumentos de cualquier naturaleza que regulen la cesión, transferencia, interconexión o acceso a datos personales entre entidades del Sector Público Nacional de conformidad con lo previsto por el artículo 8° de la Ley 24.156, vigentes al momento de

la publicación de la presente ley, deberán adecuarse a las disposiciones establecidas en la presente ley, dentro del plazo de seis (6) meses computados a partir de su publicación en el Boletín Oficial de la Nación.

Vencido el plazo previsto en el párrafo precedente, los convenios, acuerdos, protocolos o instrumentos que no se hubieren adecuado a las disposiciones de la presente ley quedarán sin efecto de pleno derecho, sin necesidad de declaración alguna.

El órgano de control podrá dictar las normas reglamentarias necesarias para supervisar el proceso de adecuación y requerir a las entidades involucradas la información que estime pertinente a tal efecto.

ARTÍCULO 16°: De forma

Juan Fernando Brügge

Diputado de la Nación

FUNDAMENTOS

Señor Presidente:

El presente proyecto de ley tiene por objeto reformar la Ley 25.326 de Protección de los Datos Personales a fin de adecuar el régimen vigente a los estándares constitucionales reafirmados por la Corte Suprema de Justicia de la Nación en la causa "Torres Abad, Carmen c/ EN – JGM s/ hábeas data" (CAF 49482/2016/CA1-CS1), resuelta en mayo de 2026.

En el pronunciamiento referido, el Máximo Tribunal de la Nación declaró la inconstitucionalidad de los artículos 5°, punto 2, inciso b y 11, punto 3, incisos b y c, de la Ley 25.326, por considerar que las excepciones al consentimiento allí previstas eran de tal generalidad que vaciaban la protección constitucional del derecho a la privacidad y a la autodeterminación informativa. La Corte señaló que, dada la amplitud con la que habían sido establecidas tales excepciones, toda la actividad estatal resultaba incluida en ellas, lo que implicaba eliminar la regla del consentimiento en un inmenso universo de situaciones.

El caso se originó en la acción de habeas data promovida por una jubilada que cuestionó un convenio mediante el cual, la Administración Nacional de la Seguridad Social (ANSES) entregaba información de su base de datos a la Secretaría de Comunicación Pública con el propósito de "mantener informada a la población". La actora argumentó que sus datos personales —entre ellos su número de teléfono y correo electrónico— habían sido recolectados para fines previsionales y que no había consentido su utilización para finalidades ajenas a las que motivaron su obtención.

La Corte reafirmó que el consentimiento del titular es la regla para la cesión de datos personales, y que el derecho a la autodeterminación informativa —esto es, el derecho de toda persona a controlar, conocer y decidir sobre el uso, almacenamiento, divulgación y actualización de sus datos personales— tiene raigambre constitucional en el artículo 43, párrafo tercero, de la Constitución Nacional. Asimismo, el Tribunal hizo especial énfasis en la dimensión del "derecho a ser dejado en paz", advirtiendo que los datos de contacto entrañan un riesgo adicional de intrusión en la esfera de tranquilidad de la persona.

La declaración de inconstitucionalidad tiene efecto inter partes, por ello que resulta imperioso que el Congreso de la Nación legisle para dar alcance general a la doctrina jurídica

sentada por la Corte Suprema, modificando las normas declaradas inconstitucionales y fortaleciendo el régimen de protección en su conjunto.

La Ley 25.326 data del año 2000 y no ha sido objeto de una actualización sustancial en más de dos décadas, pese a la transformación radical que ha experimentado el tratamiento de datos personales por parte del Estado y la evolución que a nivel mundial la temática viene teniendo. Así, las bases de datos públicas se han multiplicado, interconectado e informatizado de manera exponencial. El Estado administra hoy volúmenes de datos personales que eran inimaginables al momento de la sanción de la ley vigente: datos biométricos, datos genéticos, identificadores digitales únicos, historiales clínicos electrónicos, registros de geolocalización, entre muchos otros.

A su vez, la República Argentina aprobó mediante Ley 27.699 el Protocolo Modificatorio del Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (Convenio 108+), asumiendo el compromiso de adecuar su legislación interna a los nuevos estándares internacionales. El Convenio 108+ consagra expresamente, entre otros principios, el de la autonomía personal basada en el derecho de cada persona a controlar sus datos personales, la obligación de notificar incidentes de seguridad, la necesidad de evaluaciones de impacto previas al tratamiento de alto riesgo y la designación de órganos de control independientes con facultades efectivas. La presente reforma incorpora estos estándares a la legislación nacional.

Particular atención merece la cuestión de la seguridad de los datos personales en poder del Estado. La sucesión de incidentes de seguridad que han comprometido bases de datos públicas en los últimos años revela un cuadro de vulnerabilidad sistémica que hace urgente la reforma.

En octubre de 2021, el Registro Nacional de las Personas (RENAPER) detectó el uso indebido de credenciales de acceso otorgadas al Ministerio de Salud, a través de las cuales se extrajeron datos personales — incluyendo fotografías de documentos de identidad — de ciudadanos argentinos, que fueron luego publicados y ofrecidos a la venta en la denominada "dark web". En abril de 2024, los mismos datos resurgieron en foros de compraventa de información, incluyendo más de sesenta y cinco millones de registros del RENAPER con documentos de identidad, fotografías y datos dactiloscópicos, acompañados del código fuente, las interfaces de programación (APIs) y las credenciales de acceso a los servicios web del organismo. Simultáneamente, fueron puestas a la venta

las bases de datos de la totalidad de las licencias de conducir del país, comprometiendo datos de más de cinco millones de registros.

En diciembre de 2025, una filtración masiva de más de un terabyte de información comprometió datos provenientes de múltiples organismos públicos, incluyendo la Agencia de Recaudación y Control Aduanero (ARCA), la ANSES y registros automotores, con datos actualizados que incluían sueldos, direcciones, números de teléfono, correos electrónicos y datos vehiculares de millones de ciudadanos. La Agencia de Acceso a la Información Pública inició una investigación de oficio, aunque hasta ese momento no había recibido notificación formal de incidente de seguridad por parte de ningún organismo público, evidenciando la insuficiencia del marco regulatorio vigente en materia de notificación obligatoria.

En marzo de 2026, el grupo identificado como "Chronus Team" ejecutó un ciberataque coordinado contra la infraestructura digital del Estado argentino, con más de veintiocho filtraciones simultáneas que comprometieron bases de datos de ministerios nacionales de salud, educación y seguridad, así como de múltiples fuerzas policiales provinciales. En mayo de 2026, un nuevo actor denominado "Skull1172" anunció la filtración de datos comprometiendo más de novecientos dominios gubernamentales, universitarios y mediáticos del país.

Este historial de incidentes demuestra que las medidas de seguridad adoptadas hasta el momento por el Estado han resultado insuficientes, que los mecanismos de notificación de incidentes carecen de obligatoriedad efectiva, y que la ausencia de consecuencias sancionatorias claras para los organismos públicos que incumplen sus deberes de seguridad contribuye a la perpetuación de la vulnerabilidad de los datos de todos los argentinos. La presente reforma aborda esta problemática mediante la imposición de estándares mínimos de seguridad obligatorios, la notificación de incidentes en un plazo perentorio de setenta y dos horas, la obligatoriedad de la evaluación de impacto y la designación de delegados de protección de datos en todos los entes del Sector Público Nacional.

En cuanto al contenido de la reforma, el proyecto modifica e incorpora artículos a la Ley 25.326, manteniéndola como cuerpo normativo unificado del régimen de protección de datos personales. Las principales innovaciones son las siguientes:

Se incorporan al artículo 2° nuevas definiciones imprescindibles para la adecuación al Convenio 108+ y a la realidad tecnológica actual: dato biométrico, dato genético, identificador único e incidente de seguridad, entre otros.

Se modifica el artículo 5° para restringir la excepción al consentimiento para el ejercicio de funciones estatales, exigiendo que se trate de funciones específicas asignadas por ley y de obligaciones legales claras y precisas, en consonancia directa con lo resuelto por la Corte en Torres Abad. Se incorpora, asimismo, un principio interpretativo de particular relevancia: la invocación de competencias legales genéricas o de finalidades institucionales amplias no constituye por sí sola base legítima suficiente para el tratamiento o la cesión de datos personales sin consentimiento. Esta disposición recoge el estándar de proporcionalidad consagrado en el artículo 5.1 del Convenio 108+ y responde a la necesidad de prevenir esquemas normativos que, bajo fórmulas abiertas como la de "celebrar convenios para el cumplimiento de sus funciones" o la de "compartir información" entre organismos, habiliten en la práctica el tratamiento masivo e indiscriminado de datos personales sin control ni justificación específica. La experiencia reciente del Decreto de Necesidad y Urgencia 941/2025, que obligó a más de quince organismos públicos a compartir datos personales con la Secretaría de Inteligencia de Estado sin establecer procedimientos concretos ni mecanismos de control adecuados, ilustra con elocuencia el riesgo que esta disposición busca conjurar.

Se reformula íntegramente el artículo 11 para establecer un régimen exigente de cesión de datos entre entes públicos, con requisitos acumulativos: autorización por ley especial, finalidad compatible con la que motivó la recolección, minimización de datos y medidas de seguridad adecuadas. Se incorpora asimismo la equiparación del acceso directo, la interconexión y la interoperabilidad permanente entre bases de datos públicas a la cesión de datos, sujetándolos a las mismas condiciones. Se prohíbe la transferencia de datos personales del sector público al sector privado, salvo ejecución descentralizada de actividades públicas o autorización legal expresa.

Se moderniza el artículo 9° para imponer estándares mínimos de seguridad obligatorios —cifrado, controles de acceso, evaluación de riesgos periódica, plan de respuesta ante incidentes y capacitación del personal— a los organismos del Sector Público Nacional y a todo responsable que trate datos de más de cien mil personas. Se incorpora la obligación de notificar incidentes de seguridad al órgano de control y a los titulares de los datos en un plazo máximo de setenta y dos horas.

Se incorporan los artículos 12 bis y 12 ter, que establecen respectivamente la evaluación de impacto a la protección de datos y la figura del delegado de protección de datos, ambas instituciones previstas en el Convenio 108+ y en las mejores prácticas internacionales.

Se incorpora el artículo 22 bis, que obliga a las entidades del Sector Público Nacional a llevar un registro actualizado de todas las cesiones de datos personales efectivamente realizadas, reforzando la trazabilidad y la transparencia del tratamiento estatal.

Se reforma el régimen sancionatorio mediante la modificación del artículo 31 y la incorporación de los artículos 31 bis y 31 ter, actualizando las multas, introduciendo criterios de graduación y estableciendo un procedimiento que garantice el debido proceso.

Se amplía la legitimación activa para la acción de hábeas data, habilitando su ejercicio en representación colectiva al afectado, el Defensor del Pueblo y las organizaciones con interés legítimo, recogiendo la evolución jurisprudencial en materia de procesos colectivos y su adecuación al artículo 43 de la Constitución Nacional.

Finalmente, se establece un régimen transitorio que obliga a adecuar todos los convenios de cesión de datos vigentes entre entidades del Sector Público Nacional dentro de un plazo de seis meses, disponiendo que aquellos que no se adecuen quedarán sin efecto de pleno derecho.

El presente proyecto se inscribe en una tendencia legislativa consolidada a nivel global. El Reglamento General de Protección de Datos de la Unión Europea (RGPD), vigente desde 2018, estableció un estándar de referencia que ha sido adoptado o adaptado por legislaciones de todo el mundo, incluyendo la Lei Geral de Proteção de Dados de Brasil (Ley 13.709/2018), la Ley Federal de Protección de Datos Personales en Posesión de los Particulares de México y la Ley Marco de Protección de Datos Personales de Chile (Ley 21.719/2024). La Argentina, que fue pionera en América Latina al sancionar la Ley 25.326, debe actualizar su marco normativo para mantener los estándares de adecuación que le permiten integrar el sistema de protección de datos del Convenio 108+.

Por todo ello, solicito a los Sres. Diputados y Diputadas acompañen el presente proyecto de ley con su debida aprobación.

Juan Fernando Brügge

Diputado de la Nación