(S-0644/2025)

PROYECTO DE LEY

El Senado y Cámara de Diputados,…

LEY DE PROTECCIÓN DE LOS DATOS PERSONALES

CAPÍTULO I

DISPOSICIONES GENERALES

ARTÍCULO 1°.- Objeto. La presente Ley tiene por objeto garantizar el ejercicio del derecho fundamental de las personas humanas a la protección de sus datos personales y su privacidad.

Establece las reglas para el debido tratamiento de los datos personales y la autodeterminación informativa, así como el ejercicio de otros derechos y los deberes de quienes realizan dicho tratamiento.

ARTÍCULO 2°.- Definiciones. A los fines de la presente Ley se entiende por:

Anonimización: La aplicación de medidas dirigidas a impedir la identificación o reidentificación de una persona humana, sin esfuerzos o plazos desproporcionados, teniendo en cuenta factores como costos y tiempo necesarios para la identificación o reidentificación de la persona conforme la tecnología actual y los avances tecnológicos.

Asimismo, debe garantizarse que cualquier operación o tratamiento que se realice con posterioridad a la anonimización, no conlleve una distorsión de los datos reales.

Autodeterminación informativa: El derecho de la persona a decidir o autorizar de forma libre, previa, expresa e informada la recolección, uso o tratamiento de sus datos personales, así como de conocer, actualizar, rectificar o suprimirlos, o controlar lo que se hace con los mismos. Comprende un conjunto de principios y garantías relativas al legítimo tratamiento de sus datos personales.

Base de datos: Conjunto de datos, cualquiera sea la forma, modalidad de creación, almacenamiento, organización, tipo de soporte, tratamiento, procesamiento, localización o acceso, centralizado, descentralizado o repartido de forma funcional o geográfica. Indistintamente. Se la denomina también como archivo, registro, fichero o banco de datos.

Consentimiento de la persona Titular de los datos: Toda manifestación de voluntad previa, expresa, libre, inequívoca, informada y específica por medio de la cual la persona Titular de los datos o su representante legal, acepta, mediante una declaración o una clara acción afirmativa, que se traten sus datos personales.

Datos biométricos: Aquellos datos obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona humana, que permitan o confirmen su identificación única, tales como imágenes faciales o datos dactiloscópicos, entre otros.

Datos genéticos: Aquellos datos relativos a las características genéticas heredadas o adquiridas de una persona humana que proporcionen una información sobre su fisiología o salud.

Datos personales: Información referida a personas humanas determinadas o determinables. Se entiende por determinable, a la

persona que puede ser identificada directa o indirectamente por uno o varios elementos característicos de su identidad física, fisiológica, genética, biométrica, psíquica, económica, cultural, social o de otra índole.

Datos personales sensibles: Aquellos que se refieren a la esfera íntima de la persona Titular de los datos, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para esta. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical u opiniones políticas; datos relativos a la salud, discapacidad, orientación sexual, identidad de género, o datos genéticos o biométricos cuando puedan revelar datos adicionales cuyo uso pueda resultar potencialmente discriminatorio para la persona Titular de los datos y que estén dirigidos a identificar de manera unívoca a una persona humana.

Decisiones automatizadas: se refieren a las elecciones o conclusiones que son tomadas por sistemas de inteligencia artificial o por algoritmos sin la intervención directa de un ser humano. Estas decisiones son basadas en reglas, algoritmos o modelos de aprendizaje automático que analizan y procesan datos para determinar la acción o resultado más adecuado en una determinada situación. Se entiende por decisiones parcialmente automatizadas o semiautomatizadas a aquellas en las que no hay intervención humana significativa.

Delegado de Protección de Datos: Persona humana o jurídica encargada de informar, instruir y asesorar al Responsable o al Encargado de tratamiento sobre sus obligaciones legales en materia de protección de datos, así como de velar y supervisar el cumplimiento normativo, y de cooperar con la Autoridad de Aplicación y servir como

punto de contacto entre esta y el Responsable o Encargado de tratamiento de datos.

Elaboración de perfiles: Toda forma de tratamiento automatizado o parcialmente automatizado de datos personales consistente en utilizar estos para evaluar determinados aspectos de una persona humana; en particular, para analizar o predecir cuestiones relativas al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación, etnia, género o movimientos de dicha persona.

Encargado de tratamiento: Persona humana o jurídica, pública o privada, que trate datos personales por cuenta del Responsable de tratamiento.

Entidades crediticias: Las entidades que provean información de situación crediticia al BANCO CENTRAL DE LA REPÚBLICA ARGENTINA.

Grupo económico: Constituyen un conjunto de empresas que pueden presentarse formal y aparentemente independientes, pero sin embargo se encuentran entrelazadas al punto de formar un todo complejo compacto que responde a un mismo interés.

Incidente de seguridad de datos personales: Ocurrencia de uno o varios eventos en cualquier fase del tratamiento que atentan contra la confidencialidad, la integridad o la disponibilidad de los datos personales.

Representante de Responsable o Encargado de tratamiento: Persona humana o jurídica que ejerce la representación en el territorio nacional

de Responsables o Encargados de tratamiento que no se encuentran establecidos en la REPÚBLICA ARGENTINA.

Responsable de tratamiento: Persona humana o jurídica, pública o privada, que solo o conjuntamente con otros decide sobre la finalidad y el tratamiento de datos personales.

Seudonimización: La aplicación de medidas dirigidas a impedir que los datos personales puedan atribuirse a una persona humana sin utilizar información adicional, y que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

Tercero: Persona humana o jurídica, pública o privada, distinta de la persona Titular de los datos, del Responsable de tratamiento, del Encargado de tratamiento o de las personas autorizadas para tratar los datos personales bajo la autoridad directa del Responsable o del Encargado de tratamiento.

Titular de los datos: Persona humana cuyos datos sean objeto de tratamiento.

Transferencia internacional: La transmisión de datos personales fuera del territorio nacional.

Tratamiento de datos: Cualquier operación o conjunto de operaciones, automatizada, parcialmente automatizada o no automatizada, que se realice sobre datos personales o conjunto de datos personales. Puede implicar de manera meramente enunciativa, la recolección, registro, conservación, organización, estructuración, almacenamiento, modificación, relacionamiento, evaluación, bloqueo o destrucción,

publicación, utilización, análisis o predicción y, en general, su procesamiento, así como también su cesión a través de comunicaciones, consultas, interconexiones o transferencias.

ARTÍCULO 3°.- Ámbito de Aplicación material de la Ley. La presente Ley se aplica a todo tratamiento de datos personales realizado por una persona humana o jurídica, pública o privada, aunque los datos personales tratados no formen parte de una base de datos o se les hayan aplicado medidas de seudonimización, e incluso alcanza al tratamiento efectuado por el Estado con las finalidades de salvaguardar la seguridad pública, la defensa de la Nación, la protección de la salud pública y las libertades de terceros.

Se debe interpretar armónicamente el derecho a la protección de datos personales con el derecho a la libertad de expresión, el acceso a la información pública y el proceso de Memoria, Verdad y Justicia frente a crímenes de lesa humanidad.

En ningún caso se puede afectar el secreto de las fuentes de información periodística. Sin perjuicio de lo cual, todo otro tratamiento de los datos personales en el marco de esa actividad se encuentra alcanzado por la presente Ley.

Queda exceptuado de los alcances de la presente Ley el tratamiento de datos que efectúe una persona humana para su uso exclusivamente privado o de su grupo familiar y, por tanto, sin conexión alguna con una actividad profesional o comercial. También se exceptúa a la información anónima y a los datos anonimizados, siempre que la persona Titular de los datos no sea identificable o identificada.

ARTÍCULO 4°.- Ámbito de Aplicación territorial. La presente Ley es aplicable a cualquiera de los siguientes casos:

a) El Responsable o Encargado de tratamiento se encuentra establecido en el territorio de la REPÚBLICA ARGENTINA, aun si el tratamiento de datos tuviese lugar fuera de dicho territorio;

b) El Responsable o Encargado de tratamiento no se encuentra establecido en el territorio de la REPÚBLICA ARGENTINA, pero se da alguno de los siguientes supuestos:

I. Realiza tratamiento de datos en el territorio de la REPÚBLICA ARGENTINA mediante cualquier medio o procedimiento, físico o electrónico, actual o futuro, que le permite recolectar, usar, almacenar, indexar o tratar datos de personas que se encuentren en dicho territorio;

II. Efectúa actividades de tratamiento relacionadas con: la oferta de bienes o servicios a personas que se encuentren en el territorio de la REPÚBLICA ARGENTINA; o el perfilamiento, seguimiento o control de los actos, comportamientos o intereses de dichas personas;

III. Se encuentra establecido en un lugar en el que se aplica la legislación de la REPÚBLICA ARGENTINA en virtud del derecho internacional o de disposiciones de carácter contractual.

ARTÍCULO 5°.- Principio de neutralidad tecnológica. Esta Ley y sus normas reglamentarias se aplican a cualquier tratamiento de datos personales, con independencia de las técnicas, procesos o tecnologías, actuales o futuras, que se utilicen para dicho efecto.

CAPÍTULO II

TRATAMIENTO DE DATOS PERSONALES

ARTÍCULO 6º.- Principio de licitud, lealtad y transparencia. El tratamiento se considera lícito si se realiza conforme la legislación vigente. Se considera leal si el tratamiento es honesto y sin engaños o fraudes.

Es transparente si la información vinculada al tratamiento de los datos es fácilmente accesible y utiliza un lenguaje sencillo y claro.

ARTÍCULO 7º.- Principio de finalidad. Los datos personales deben ser recogidos con fines determinados, explícitos y legítimos, y su tratamiento ulterior debe ser compatible con dichos fines.

Se considera compatible el tratamiento en archivos con fines de investigación histórica de interés público.

ARTÍCULO 8º- Principio de minimización de datos. Los datos personales deben ser tratados de manera que sean adecuados, pertinentes y limitados a lo necesario, en relación con los fines para los que fueron recolectados.
A solicitud de la Autoridad de Aplicación, los Responsables de tratamiento deberán proveer una justificación de la necesidad de tratar los datos en cada caso.

ARTÍCULO 9º.- Principio de exactitud, integridad y confidencialidad. Los datos personales objeto de tratamiento deben ser veraces, exactos, completos, comprobables y actualizados.

Se deberán adoptar todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.

Se prohíbe el tratamiento de datos falsos, desactualizados, inexactos, incompletos o que induzcan a error.

Se presume la exactitud de los datos proporcionados por su titular.

El tratamiento se considera íntegro y confidencial, si los datos personales son tratados de manera que se garantice una seguridad adecuada de los mismos, mediante la aplicación de medidas técnicas u organizativas apropiadas.

ARTÍCULO 10.- Principio de preeminencia. En caso de duda sobre la interpretación y la aplicación de la presente Ley, prevalecerá la más favorable a la persona Titular de los datos personales.

ARTÍCULO 11.- Principio de limitación del plazo de conservación. Los datos personales no deben ser mantenidos más allá del tiempo estrictamente necesario para el cumplimiento de la finalidad del tratamiento. Pueden conservarse durante períodos más largos siempre que se trate exclusivamente de fines estadísticos, de archivo en interés público, de investigación científica o histórica, y se apliquen las medidas técnicas y organizativas apropiadas que impone la presente Ley.

ARTÍCULO 12.- Principio de responsabilidad proactiva y demostrada. El Responsable y el Encargado de tratamiento deben adoptar las medidas técnicas, organizativas o de cualquier otra índole que sean útiles, oportunas y efectivas con el fin de garantizar un tratamiento adecuado de los datos personales, el cumplimiento de las obligaciones dispuestas

por la presente Ley y ser capaces de demostrar a la Autoridad de Aplicación su efectiva implementación.

El Responsable y el Encargado de tratamiento se encuentran obligados a la implementación de la debida diligencia en la materia, entendida como un proceso continuo, orientado a identificar, prevenir, rendir cuentas y mitigar los impactos adversos que se pudieran ocasionar.

ARTÍCULO 13.- Bases legales para el tratamiento de datos. El tratamiento de datos personales sólo puede realizarse si se cumple al menos una de las siguientes bases legales:

a) Que la persona Titular de los datos otorgue su consentimiento para uno o varios fines específicos;

b) Que se efectúe en ejercicio de las funciones y facultades propias de los poderes del Estado y sean necesarios para el cumplimiento de sus competencias;

c) Que sea necesario para el cumplimiento de una obligación legal aplicable al Responsable o al Encargado de tratamiento;

d) Que sea necesario para la ejecución de un contrato en el que la persona Titular de los datos sea parte, o para la aplicación de medidas precontractuales;

e) Que resulte necesario para salvaguardar la vida de la persona Titular de los datos o de terceros;

f) Que sea necesario para la satisfacción del interés legítimo del Responsable de tratamiento, siempre que sobre dicho interés no prevalezcan los intereses o los derechos de la persona Titular de los

datos, en particular si la persona Titular de los datos es una niña, un niño o adolescente.

Para fundamentar la existencia de un interés legítimo que justifique la necesidad del tratamiento de datos personales, el Responsable de tratamiento debe realizar un análisis detallado, previo y documentado, que incluya el contexto y las circunstancias en las que se llevará a cabo el tratamiento y el nivel de riesgo que implica. En este caso, deberá reforzarse el respeto del principio de minimización de datos y su tratamiento deberá acotarse sobre la base de criterios expresos de proporcionalidad y razonabilidad.

En el marco de los procesos de control, la Autoridad de Aplicación podrá requerir al Responsable de tratamiento el análisis previo referido, teniendo para sí la carga de la prueba que demuestre la existencia del interés legítimo, la necesidad de recolección y tratamiento, como así los criterios aplicados.

ARTÍCULO 14.- Consentimiento. En el caso en que la base legal para el tratamiento de datos sea el consentimiento de la persona Titular de los datos, se requiere que este sea expreso, previo, libre, específico, informado e inequívoco, para una o varias finalidades determinadas, ya sea mediante una declaración o una clara acción afirmativa.
Se entiende por:

a) Previo, cuando se solicita el consentimiento antes de la recolección de los datos;

b) Expreso, cuando la persona Titular de los datos exterioriza su voluntad con una clara acción afirmativa;

c) Libre, cuando se encuentra exento de vicios. La persona Titular de los datos debe tener la opción de negarse a otorgar su consentimiento sin sufrir perjuicio alguno;

d) Específico, cuando, en el caso que el tratamiento tenga varios fines, la persona Titular de los datos se encuentra posibilitada de otorgar su consentimiento para cada uno de ellos;

e) Informado, cuando la persona Titular de los datos cuenta con la información establecida en el artículo 16 de esta Ley;

f) Inequívoco, cuando no presente dudas sobre el alcance de la autorización otorgada por la persona Titular de los datos.

En ningún caso, podrá entenderse que el consentimiento ha sido otorgado de manera tácita o presunta.

El Responsable de tratamiento debe ser capaz de demostrar que la persona Titular de los datos consintió el tratamiento de sus datos personales.

ARTÍCULO 15.- Revocación del consentimiento. La persona Titular de los datos puede revocar el consentimiento en cualquier momento y sin necesidad de fundamentar.

La revocación no tiene efectos retroactivos.

El Responsable de tratamiento debe proveer para la revocación mecanismos sencillos, gratuitos, expeditos y con la misma facilidad con la que obtuvo el consentimiento.

ARTÍCULO 16.- Información a la persona Titular de los datos. El Responsable de tratamiento debe brindar a la persona Titular de los datos, antes de la recolección, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, como mínimo la siguiente información:

a) Nombre o razón social, domicilio y medios electrónicos del Responsable y del Encargado de tratamiento; en su caso, del Delegado de Protección de Datos y, en el supuesto de los Responsables o Encargados de tratamiento no establecidos en el país, los de su Representante en el territorio nacional;

b) Las categorías de datos personales que serán objeto del tratamiento;

c) Las finalidades que se persiguen con el tratamiento de los datos y las bases legales de este;

d) Los derechos de la persona Titular de los datos y los medios, procedimientos y persona o área responsable para su ejercicio;

e) Toda información sobre cesiones a otros Responsables o Encargados de tratamiento;

f) Aquella información sobre las transferencias internacionales de datos, con inclusión de países de destino, identidad y datos de contacto del destinatario, posibles riesgos asociados a las transferencias y salvaguardas aplicables, categorías de datos involucradas, finalidad y mecanismos para ejercer sus derechos;

g) El carácter obligatorio o facultativo de proporcionar los datos personales y las consecuencias de proporcionarlos, o de la negativa a hacerlo, o de hacerlo en forma incompleta o defectuosa;

h) El derecho de la persona Titular de los datos a revocar el consentimiento;

i) El plazo durante el cual se conservarán los datos personales o, si esto no es posible, los criterios utilizados para determinar este plazo;

j) La existencia o no de decisiones automatizadas o semiautomatizadas, incluida la elaboración de perfiles;

k) El derecho a presentar una denuncia, a iniciar el trámite de protección de datos personales ante la Autoridad de Aplicación, o a ejercer la acción de hábeas data.

l) La posibilidad de ejercer los derechos de acceso, rectificación, oposición, supresión y portabilidad de los datos.

El Responsable de tratamiento tiene la obligación de proveer a la persona Titular de los datos la información prevista en el presente artículo, incluso si no ha obtenido la información directamente de ella, o si no se ha tomado su consentimiento como base legal para legitimar dicho tratamiento.

Si los datos no han sido obtenidos de la persona Titular, el Responsable de tratamiento debe proveer la información prevista en el presente artículo dentro de un plazo razonable que no puede exceder de UN (1) mes desde que los ha obtenido.

En los casos en que los datos se utilicen para comunicarse con la persona Titular se debe proveer la información al momento de la primera comunicación, y si son cedidos a otro destinatario se debe informar en la primera cesión.

ARTÍCULO 17.- Tratamiento de datos sensibles.

Se prohíbe el tratamiento de datos sensibles, excepto si:

a) La persona Titular de los datos ha dado su consentimiento a dicho tratamiento;

b) Fuera necesario para salvaguardar la vida de la persona Titular de los datos y esta se encontrara imposibilitada para prestar el consentimiento por sí o por sus representantes;

c) Es efectuado por instituciones sanitarias públicas o privadas o por profesionales o agentes de la salud con la finalidad de brindar un tratamiento de salud específico y de acuerdo a lo establecido por la Ley Nº 26.529 y sus modificatorias de DERECHOS DEL PACIENTE, HISTORIA CLÍNICA Y CONSENTIMIENTO INFORMADO.

Se prohíbe a los operadores de planes privados de salud tratar datos de salud para la práctica de selección de riesgo en la contratación de cualquier modalidad y la exclusión de beneficiarios;

d) Se realiza en el marco de las actividades legítimas de una fundación, asociación o cualquier otro organismo sin fines de lucro, cuyo objeto principal sea una actividad política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente al registro de sus miembros o de las personas que mantengan un contacto regular por razón de su

objeto principal, y que los datos personales no se comuniquen fuera de ellos;

e) Se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial o administrativo;

f) Tuviera una finalidad histórica, de archivo de interés público, de aporte al proceso de Memoria, Verdad y Justicia frente a crímenes de lesa humanidad en cuyo caso deberán adoptarse, en la medida de lo posible, un procedimiento de anonimización o seudonimización;

g) Tuviera una finalidad estadística o científica, siempre que la persona Titular de los datos no pueda ser identificada;

h) Fuera necesario para el cumplimiento de obligaciones legales del Responsable de tratamiento o del ejercicio de derechos de la persona Titular de los datos en el ámbito del derecho laboral y de la seguridad social, la salud pública y la protección social;

i) Fuera necesario en ejercicio de las funciones y facultades de los Poderes del Estado en el cumplimiento estricto de sus competencias;

j) Se realiza en el marco de la asistencia humanitaria.

Se prohíbe el tratamiento de datos sensibles que conlleve perjuicio o discriminación hacia la persona Titular de datos personales.

En el tratamiento de datos sensibles se debe implementar la responsabilidad reforzada que implica, entre otras características, mayores niveles y condiciones más estrictas de seguridad, confidencialidad, restricciones de acceso, uso y circulación, lo que debe

implementarse mediante salvaguardas apropiadas adicionales y diseñadas específicamente.

ARTÍCULO 18.- Tratamiento de datos del sector público.

El tratamiento de datos personales realizado por el sector público debe fundarse en las bases legales y cumplir con todos los principios y condiciones que definen la licitud para el tratamiento.

Las cesiones de datos personales efectuadas por organismos del Sector Público deben implementarse mediante un acuerdo entre cedente y cesionario. El Responsable de tratamiento cesionario queda sujeto a las mismas obligaciones legales y reglamentarias que el Responsable de tratamiento cedente. Ambos responden por la observancia de aquellas ante la Autoridad de Aplicación y ante la persona Titular de los datos.

El acuerdo debe respetar el principio de máxima publicidad y disponibilidad, y debe contener: las finalidades, la categoría de datos personales, la base que legitima el tratamiento, los plazos de conservación, medidas de seguridad y toda otra información que determine la Autoridad de Aplicación.

El Sector Público tiene la obligación de documentar los procedimientos establecidos para el tratamiento de los datos personales, e implementar planes de protección de datos personales y de formación y capacitación en la materia para su personal, así como establecer mejoras de infraestructura y medidas de seguridad acordes al volumen y el carácter de los datos tratados.

Esta ley es aplicable al tratamiento de datos personales efectuado por las Fuerzas Armadas, fuerzas de seguridad y de inteligencia. Cualquier medida que imponga una limitación a los derechos y garantías

establecidos en la presente ley, debe ser necesaria y proporcional, tener en cuenta los intereses legítimos del Titular de los datos, establecer salvaguardias y respetar los derechos fundamentales consagrados en la CONSTITUCIÓN NACIONAL.

ARTÍCULO 19.- Tratamiento de datos de niñas, niños y adolescentes. En el tratamiento de datos personales de niñas, niños y adolescentes, debe prevalecer el interés superior de los mismos.

Es válido el consentimiento de adolescentes a partir de DIECISÉIS (16) años para el tratamiento de sus datos personales, con excepción de los alcanzados por el artículo 22 de la Ley N° 26.061, su Decreto Reglamentario y demás normativa aplicable.

En el caso de niñas, niños y adolescentes menores de DIECISÉIS (16) años, pueden dar su asentimiento informado, pero el tratamiento únicamente se considerará lícito si la persona titular de la responsabilidad parental o quien se encuentre a cargo de su ejercicio o de la guarda o tutela sobre la niña, el niño o adolescente sea quien otorgue el consentimiento. En tales casos, el Responsable de tratamiento deberá arbitrar procesos que permitan verificar dicho cumplimiento.

La información sobre el tratamiento de datos a que se refiere este artículo debe ser brindada de forma simple, clara y accesible, considerando las características físico-motoras, perceptivas, sensoriales, intelectuales, mentales y adecuado a la comprensión del menor o adolescente, de modo tal que el niño o niña pueda dar su asentimiento o consentimiento informado.

Se prohíbe realizar el tratamiento de datos personales de niños, niñas y adolescentes en los juegos, aplicaciones, desarrollos e innovaciones

tecnológicas, u otras actividades afines que involucren información personal, más allá de lo estrictamente necesario para la realización de la actividad.

Se prohíbe tratar datos sensibles de niñas, niños y adolescentes, a menos que:

a) se cuente con el consentimiento de la persona titular de la responsabilidad parental o de quien se encuentre a cargo de su ejercicio o de la guarda o tutela de la niña, del niño o adolescente;

b) el tratamiento fuera indispensable para salvaguardar la vida de aquellos, siempre que la persona titular de la responsabilidad parental o de quien se encuentre a cargo de su ejercicio o de la guarda o tutela de niña, niño o adolescente estuviere imposibilitada para prestar el consentimiento.

El Estado a través de las áreas correspondientes debe proveer información y capacitar a niñas, niños y adolescentes sobre los eventuales riesgos a los que se enfrentan respecto del tratamiento indebido de sus datos personales, sobre el uso responsable y seguro de sus datos personales, sobre su derecho a la privacidad y a la autodeterminación informativa, y sobre el respeto de los derechos de los demás.

ARTÍCULO 20.- Sistema de administración de riesgos. El Responsable y el Encargado de tratamiento de datos personales deben sujetarse al principio de integridad y confidencialidad de los datos personales, para lo cual deben adoptar las medidas técnicas, organizativas y de cualquier otra naturaleza que resulten apropiadas para garantizar la seguridad de los datos personales, para evitar su adulteración, pérdida, uso, consulta 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.

Para ello deben adoptar un sistema de administración de riesgos asociados y tomar en cuenta las categorías y volumen de los datos personales, la probabilidad de riesgos, el estado de la técnica, las mejores prácticas de seguridad integral y los costos de aplicación de acuerdo a la naturaleza, el alcance, el contexto y los fines del tratamiento.

Deben adoptar las medidas de seguridad aplicables a los datos personales que trate, considerar los siguientes factores como mínimo y que las medidas adoptadas eviten la materialización de los riesgos identificados:

a) El riesgo inherente por el tipo de dato personal;

b) El carácter sensible de los datos personales tratados;

c) El desarrollo tecnológico;

d) Las posibles consecuencias de un incidente de seguridad para las personas Titulares de los datos;

e) Los incidentes de seguridad previos ocurridos en los sistemas de tratamiento.

ARTÍCULO 21.- Notificación de incidentes de seguridad de datos personales. En caso de que ocurra un incidente de seguridad de los datos personales, el Responsable de tratamiento debe notificarlo a la Autoridad de Aplicación dentro de las SETENTA Y DOS (72) horas de haber tomado conocimiento de aquel. En caso de no contar con los

medios materiales para cumplir con la notificación en el plazo previsto, deberá solicitar a la Autoridad de Aplicación prórroga debidamente fundada.

Asimismo, deberá informar a la persona Titular de los datos sobre el incidente de seguridad ocurrido, en un lenguaje claro y sencillo. Si ello supone un esfuerzo desproporcionado, dicha notificación puede realizarse mediante una comunicación pública.

La notificación debe contener, como mínimo la siguiente información:

a) La naturaleza del incidente;

b) Los datos personales que pueden estimarse comprometidos;

c) Las acciones correctivas realizadas de forma inmediata;

d) Las recomendaciones a la persona Titular de los datos acerca de las medidas que este puede adoptar para proteger sus intereses y derechos;

e) Los medios a disposición de la persona Titular de los datos para obtener mayor información al respecto, incluido el nombre y datos de contacto del Delegado de Protección de Datos o cualquier otra persona o área designada como contacto.

En caso de que no sea posible enviar toda la información detallada al mismo tiempo, el Responsable de tratamiento deberá enviarla a medida que sea posible y sin dilación alguna que le sea imputable.

El Responsable de tratamiento debe documentar todo incidente de seguridad que ponga en alto riesgo los derechos de las personas

Titulares de los datos, ocurrido en cualquier fase del tratamiento de datos e identificar, de manera enunciativa pero no limitativa, la fecha en que ocurrió, el motivo del incidente, los hechos relacionados con este y sus efectos, y las medidas correctivas implementadas de forma inmediata y en definitiva.

ARTÍCULO 22.- Deber de confidencialidad. El Responsable de tratamiento, el Encargado y las demás personas que intervengan en cualquier fase de tratamiento de datos personales, están sujetas al deber de confidencialidad, el cual subsiste aun después de finalizada la relación con la persona Titular.

El obligado puede ser relevado del deber de confidencialidad por resolución judicial u obligación legal.

CAPÍTULO III

TRANSFERENCIAS INTERNACIONALES

ARTÍCULO 23.- Principio general de las transferencias internacionales. Las transferencias de datos personales fuera del territorio nacional, incluidas las transferencias ulteriores, se pueden realizar en cualquiera de los siguientes supuestos:

a) Si el país u organismo internacional o supranacional receptor proporciona un nivel de protección adecuado;

b) Si el Responsable o Encargado de tratamiento exportador ofrece garantías apropiadas al tratamiento de los datos personales, en cumplimiento de las condiciones mínimas y suficientes establecidas en esta Ley;

c) Si se configuran las excepciones para situaciones específicas determinadas en el artículo 26 de la presente Ley.

En todos los casos, recae en el Responsable o Encargado de tratamiento exportador la carga de la prueba a efectos de demostrar que la transferencia internacional se efectúa conforme esta ley.
Asimismo debe implementar medidas para garantizar los derechos de las personas Titulares de los datos y responder frente a su eventual vulneración.

ARTÍCULO 24.- Transferencias internacionales basadas en una decisión de adecuación. La Autoridad de Aplicación será quien determine, a los fines del inciso a) del artículo 23 la condición de adecuado, teniendo en cuenta los siguientes elementos:

a) El estado de derecho, el respeto de los derechos humanos y las libertades fundamentales;

b) La legislación vigente, tanto general como sectorial, incluidas las limitaciones y garantías para el acceso de las autoridades públicas a los datos personales;

c) La existencia de garantías judiciales e institucionales para la protección de datos personales y privacidad;

d) La existencia y el funcionamiento efectivo de una o varias autoridades de control independientes que reciban la información, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a las personas Titulares de los datos en el ejercicio de sus derechos, y de cooperar con la Autoridad de Aplicación.

ARTÍCULO 25.- Transferencias internacionales mediante garantías adecuadas. A los fines del inciso b) de artículo 23, las garantías adecuadas pueden ser aportadas por:

a) Un instrumento jurídicamente vinculante y exigible entre autoridades u organismos públicos de la REPÚBLICA ARGENTINA y de otros países, que contenga los principios, derechos y obligaciones establecidos en la presente Ley;

b) Un acuerdo internacional bilateral o multilateral, entre la REPÚBLICA ARGENTINA y otros países u organizaciones internacionales, que contenga los principios, obligaciones y derechos establecidos en la presente Ley, y que habilite las transferencias desde entidades privadas y/o públicas establecidas en la REPÚBLICA ARGENTINA hacia entidades privadas y/o públicas establecidas en otros países;

c) Acuerdos o convenios que expresamente reconozcan los principios, derechos y obligaciones establecidos en la presente Ley, los que pueden adoptar las siguientes formas:

I. Cláusulas contractuales modelo que hayan sido previamente aprobadas por la Autoridad de Aplicación;

II. Normas corporativas vinculantes que hayan sido aprobadas por la Autoridad de Aplicación y que se apliquen a todos los miembros de un grupo económico;

III. Mecanismos de certificación en materia de protección de datos aprobados por la Autoridad de Aplicación.

El acuerdo o mecanismo que instrumente la transferencia, debe reconocer que el Responsable o Encargado de tratamiento exportador se encuentra sujeta a la jurisdicción de la Autoridad de Aplicación y de los tribunales de la REPÚBLICA ARGENTINA competentes y asegurar que el Responsable o Encargado de tratamiento importador se encuentre sujeta a la jurisdicción de una o varias autoridades de supervisión independientes de manera que las personas Titulares de los datos cuenten con acciones legales y administrativas efectivas para proteger sus derechos.

ARTÍCULO 26 - Excepciones. A los fines del inciso c) de artículo 23, las transferencias internacionales pueden realizarse por excepción si se cumple alguna de las siguientes condiciones:

a) Que la persona Titular de los datos haya otorgado su consentimiento;

b) Que la transferencia sea necesaria para la ejecución de un contrato entre la persona Titular de los datos y el Responsable de tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud de la persona Titular de los datos;

c) Que la transferencia sea necesaria:

I. Por razones de interés público;

II. Para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial;

III. Para proteger la vida de la persona Titular de los datos o de otras personas.

Las excepciones enumeradas en el presente artículo no pueden ser utilizadas para realizar transferencias internacionales de forma periódica o habitual, ni que involucren a un gran número de personas.

CAPÍTULO IV

DERECHOS DE LOS TITULARES DE LOS DATOS

ARTÍCULO 27.- Derecho de acceso. La persona Titular de los datos, previa acreditación de su identidad, tiene el derecho a saber si se están tratando sus datos personales.

También le asiste el derecho de acceso a sus datos, así como a conocer cualquier información relacionada con las condiciones generales y específicas de su tratamiento.

De manera específica, pero no excluyente, tiene derecho a obtener la siguiente información sobre el tratamiento de sus datos:

a) Las finalidades del tratamiento y las bases legales que legitiman cada finalidad;

b) Las categorías de datos personales que se tratan;

c) Los destinatarios o las categorías de destinatarios a los que se cedieron o se prevean ceder los datos personales;

d) Lo relativo a las transferencias internacionales de datos que se hayan efectuado o se prevea efectuar, con inclusión de países de destino y base legal que justifica la transferencia;

e) El plazo previsto de conservación de los datos personales o, de no ser ello posible, los criterios utilizados para determinar este plazo;

f) El derecho a solicitar la rectificación o la supresión de datos personales, así como a oponerse a dicho tratamiento;

g) El derecho a iniciar un trámite de protección de datos personales ante la Autoridad de Aplicación;

h) Cualquier información disponible sobre el origen de los datos personales cuando no hayan sido obtenidos de la persona Titular de los datos;

i) La existencia de decisiones automatizadas, incluida la elaboración de perfiles a que se refiere el artículo 31 de la presente Ley, en cuyo caso, como mínimo debe indicarse la información significativa y suficiente para que la persona Titular de los datos comprenda cómo se toman las decisiones y se llega a los resultados y sus posibles consecuencias;

j) El derecho a no ser objeto de decisiones individuales automatizadas y todo otro derecho que surja de la normativa específica.

En ningún caso, el informe puede revelar datos pertenecientes a terceros, aún si se vinculan con la persona Titular de los datos. La información, a opción de la persona Titular de los datos, puede entregarse por escrito, por medios electrónicos, telefónicos, de imagen u otro idóneo a tal fin.

Toda la información debe ser suministrada en forma accesible, de fácil comprensión, completa, exenta de codificaciones y acompañada de una explicación de los términos que se utilicen.

Este derecho puede ser ejercido en forma gratuita a intervalos superiores a SEIS (6) meses. En el caso de intervalos inferiores, el Responsable de tratamiento puede cobrar un monto razonable en función de los costos administrativos afrontados para facilitar la información a la persona Titular de los datos.

ARTÍCULO 28.- Derecho de rectificación. La persona Titular de los datos tiene el derecho a obtener del Responsable de tratamiento la rectificación de sus datos personales cuando estos resulten ser inexactos, falsos, erróneos, incompletos o desactualizados.

En el supuesto de cesión o transferencia internacional de datos erróneos o desactualizados, el Responsable de tratamiento debe notificar la rectificación al cesionario o importador dentro del plazo de CINCO (5) días hábiles de haber tomado conocimiento efectivo del error o la desactualización.

Durante el proceso de verificación y rectificación de la información de que se trate, el Responsable de tratamiento debe bloquear el dato, o bien consignar, al proveer información relativa a este, la circunstancia de que se encuentra sometido a revisión.

ARTÍCULO 29.- Derecho de oposición. La persona Titular de los datos puede oponerse al tratamiento, 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, salvo que existan motivos legítimos para el tratamiento que prevalezcan sobre los derechos de la persona Titular de los datos.

La persona Titular de los datos también puede oponerse si tuvieran por objeto la publicidad, la prospección comercial o la mercadotecnia directa, incluida la elaboración de perfiles. En este caso, sus datos personales deben dejar de ser tratados.

El tratamiento de datos personales debe limitarse a su almacenamiento durante el período que medie entre una solicitud de oposición hasta su resolución por el Responsable de tratamiento.

ARTÍCULO 30.- Derecho de supresión. La persona Titular de los datos tiene derecho a solicitar la supresión de sus datos personales al Responsable de tratamiento. La supresión procede si:

a) Los datos personales ya no son necesarios en relación con los fines para los que fueron recolectados;

b) La persona Titular de los datos revoca el consentimiento en que se basa el tratamiento de datos y este no se ampara en otra base legal;

c) La persona Titular de los datos ha ejercido su derecho de oposición conforme al artículo 29 de esta Ley, y no prevalecen otros motivos legítimos para el tratamiento de sus datos;

d) Los datos personales hayan sido tratados ilícitamente;

e) Los datos personales deban suprimirse para el cumplimiento de una obligación legal o por orden de autoridad competente;

f) Los datos son tratados para fines de publicidad, prospección comercial o mercadotecnia.

La supresión no procede si pudiese causar perjuicios a derechos de terceros, si prevalecen razones de interés público para el tratamiento de datos cuestionado, o si los datos personales deben ser conservados durante los plazos previstos en las disposiciones legales aplicables o, en su caso, en las cláusulas contractuales acordadas entre el Responsable o Encargado de tratamiento y la persona Titular de los datos.

Tampoco procede si el dato es necesario para el esclarecimiento de casos de violaciones de derechos humanos, genocidio, crímenes de guerra o delitos de lesa humanidad.

ARTÍCULO 31.- Decisiones automatizadas y elaboración de perfiles. La persona Titular de los datos tiene derecho a no ser objeto de una decisión que le produzca efectos jurídicos perniciosos, lo afecte de forma negativa o tengan efectos discriminatorios, basada, única o parcialmente, en el tratamiento automatizado de datos, incluida la elaboración de perfiles.

El Responsable de tratamiento debe proporcionar, siempre que se le solicite, información clara, completa y adecuada sobre los criterios y procedimientos utilizados para la decisión automatizada o semiautomatizada, con observancia de secretos comerciales e industriales.

En caso de no proporcionar la información con base en la observancia del secreto comercial e industrial, la Autoridad de Aplicación puede realizar auditorías para verificar, entre otros, aspectos discriminatorios o de contenido erróneo o sesgado en el tratamiento automatizado o semiautomatizado de los datos personales.

El Responsable de tratamiento debe adoptar las medidas adecuadas para salvaguardar los derechos de la persona Titular de los datos; como mínimo, debe garantizar:

a) Explicabilidad y documentación de sus algoritmos.

b) Auditorías y certificaciones externas para garantizar transparencia y cumplimiento de la presente.

c) Supervisión humana en sistemas automatizados de alto impacto en los derechos de las personas.

d) Publicación de informes periódicos sobre la utilización de algoritmos en procesos que afecten a las personas.

e) Implementación de mecanismos de reclamación y revisión para las personas Titulares de datos afectadas por decisiones automatizadas.

f) Brindar las explicaciones de las decisiones tomadas por sistemas de algoritmos ante el requerimiento de la persona afectada.

Sin perjuicio de lo que establezca la normativa específica, la persona Titular de los datos, tiene derecho a solicitar la revisión por una persona humana de las decisiones tomadas sobre la base del tratamiento automatizado o semiautomatizado que afecten a sus intereses, incluidas las decisiones encaminadas a definir sus aspectos personales, profesionales, de consumo, de crédito, de su personalidad u otros.

El Responsable de tratamiento no puede llevar a cabo tratamientos automatizados o semiautomatizados de datos personales que tengan como efecto la discriminación en detrimento de las personas Titulares de los datos, perpetuar situaciones que afecte a la diversidad y la

inclusión, o violar derechos humanos fundamentales como la privacidad, la libertad de expresión, la igualdad o la dignidad humana.

También se prohíbe el tratamiento cuando es utilizado para manipular o influir de manera indebida en la toma de decisiones importantes, como en procesos electorales o en la formación de opiniones públicas, atentando contra la integridad y la legitimidad de dichos procesos.

ARTÍCULO 32.- Derecho a la portabilidad de datos personales. Si se tratan datos personales mediante medios electrónicos o automatizados, la persona Titular de los datos tiene derecho a obtener una copia de los datos personales que hubiere proporcionado al Responsable de tratamiento o que sean objeto de tratamiento, en un formato que le permita su ulterior utilización por parte de otro Responsable de Tratamiento.

La persona Titular de los datos puede solicitar que sus datos personales se transfieran directamente de Responsable a Responsable de tratamiento si ello fuera técnicamente posible.

Este derecho no procede si:

a) Su ejercicio impone una carga financiera o técnica excesiva o irrazonable sobre el Responsable de tratamiento, de conformidad con lo que establezca la normativa complementaria;

b) Vulnera la privacidad de otra persona Titular de los datos;

c) Afecta las obligaciones legales del Responsable de tratamiento;

d) Impide que el Responsable de tratamiento proteja sus derechos, seguridad, bienes, o los del Encargado de tratamiento, o de la persona Titular de los datos o de un tercero.

El derecho a la portabilidad no es procedente si se trata de información inferida, derivada, creada, generada u obtenida a partir del análisis o tratamiento efectuado por el Responsable de tratamiento.

ARTÍCULO 33.- Derecho de limitación. La persona Titular de los datos tiene derecho a obtener del Responsable de tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:

a) Si impugna la exactitud de los datos personales, durante un plazo que permita al Responsable de tratamiento verificar la exactitud de los mismos;

b) Si el tratamiento es ilícito y se opone a la supresión de los datos personales y solicita en su lugar la limitación de su uso;

c) Si el Responsable de tratamiento ya no necesita los datos personales para los fines del tratamiento, pero los necesita para el ejercicio o la defensa de sus derechos;

d) Si se ha opuesto al tratamiento en virtud del artículo 29 de la presente Ley, mientras se verifica si prevalecen los motivos legítimos del Responsable de tratamiento

En caso de negativa a la limitación, el Titular de los datos podrá recurrir a la Autoridad de Aplicación y en dicho caso, la limitación se extenderá hasta la resolución del procedimiento administrativo.

El Responsable de tratamiento antes del levantamiento debe informar a la persona Titular de los datos.

ARTÍCULO 34.- Ejercicio de los derechos. El ejercicio de cualquiera de los derechos de la persona Titular de los datos no es requisito previo ni impide el ejercicio de otro. Son irrenunciables y toda estipulación en contrario es nula de pleno derecho. El Responsable de tratamiento debe responder y, en su caso, satisfacer el pedido de la persona Titular de los datos dentro de los DIEZ (10) días hábiles de haber sido intimado fehacientemente.

Vencido el plazo sin que se satisfaga el pedido, o si a juicio de la persona Titular de los datos la respuesta se estimara insuficiente, quedará expedito el trámite de protección de los datos personales ante la Autoridad de Aplicación en los términos del artículo 56 o, a elección de la persona Titular de los datos, la acción de Habeas Data prevista en el artículo 66, ambos de la presente. En caso de optar por esta última, o de haberla iniciado con anterioridad, no puede iniciar el trámite de protección ante la Autoridad de Aplicación.

En caso de fallecimiento de la persona Titular de los datos, el ejercicio de los derechos, corresponde a sus sucesores universales.

El Responsable de tratamiento debe establecer medios y procedimientos sencillos, expeditos, accesibles y gratuitos que permitan a la persona Titular de los datos ejercer los derechos previstos en esta Ley.

La persona Titular de los datos tiene derecho a reclamar en sede judicial una indemnización por los daños y perjuicios sufridos como consecuencia de una infracción a la presente Ley.

El ejercicio abusivo de los derechos por parte de la persona Titular de los datos no se encuentra amparado. Se considera tal el que contraría los fines de la presente Ley, excede los límites impuestos por la buena fe o resulta manifiestamente infundado o excesivo. Recae en el Responsable del tratamiento la carga de la prueba a efectos de demostrar el ejercicio abusivo.

ARTÍCULO 35.- Excepciones al ejercicio de los derechos. Los derechos y las garantías establecidos pueden ser limitados en la medida en que ello sea necesario y proporcional para salvaguardar la seguridad pública, la defensa de la Nación, la protección de la salud pública, y las libertades de terceros y en resguardo del interés público.

Las limitaciones y restricciones generales deben ser reconocidas de manera expresa mediante una norma de rango legal y debe contener, como mínimo, disposiciones relativas a:

a) La finalidad del tratamiento;

b) Las categorías de datos personales de que se trate;

c) El alcance de las limitaciones establecidas;

d) Los plazos de conservación de los datos personales;

e) La determinación del Responsable o de los Responsables de tratamiento;

f) Los posibles riesgos para los derechos y libertades de las personas Titulares de los datos;

g) El derecho de las personas Titulares de los datos a ser informados sobre la limitación, salvo que resulte perjudicial o incompatible a los fines de esta.

También, pueden establecerse limitaciones específicas si existe una orden fundada, dictada por autoridad judicial o administrativa competente, en los casos en que se pudieran obstaculizar actuaciones vinculadas a investigaciones en el marco de sus facultades.

CAPÍTULO V

OBLIGACIONES DE LOS RESPONSABLES Y ENCARGADOS DE TRATAMIENTO

ARTÍCULO 36.- Deberes del Responsable de tratamiento. Los Responsables de tratamiento deben cumplir los siguientes deberes:

a) Implementar medidas apropiadas, útiles, oportunas, pertinentes y eficaces para garantizar y poder demostrar el adecuado cumplimiento de la presente Ley y las normas reglamentarias;

b) Garantizar a la persona Titular de los datos, en todo tiempo, el pleno y efectivo ejercicio de los derechos reconocidos en la presente;

c) Cumplir con el deber de informar a la persona Titular de los datos sobre la finalidad de la recolección y sus derechos;

d) Tratar los datos personales bajo condiciones de seguridad apropiadas para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

e) Implementar medidas para garantizar que los datos personales sean veraces, actualizados, completos, exactos y comprobables;

f) Actualizar los datos personales, rectificar la información si fuera incorrecta y adoptar medidas necesarias para que esta se mantenga actualizada;

g) Tramitar las solicitudes presentadas por la persona Titular de los datos, y responderlas de manera completa y oportuna;

h) Notificar en el plazo de ley los incidentes de seguridad ocurridos, de acuerdo al artículo 21 de la presente Ley;

i) Cumplir las instrucciones, órdenes o requerimientos que imparta la Autoridad de Aplicación;

j) Formalizar mediante la suscripción de un acuerdo, contrato o cualquier otro instrumento jurídico la prestación de servicios con el Encargado de tratamiento.

k) Verificar que los Encargados de tratamiento, o quienes estos subcontraten, ofrezcan garantías suficientes para realizar el tratamiento de datos personales y garanticen la protección de los derechos de la persona Titular de los datos; dicha verificación debe realizarse con anterioridad a la contratación o realización de otro acto jurídico que lo vincule con el Encargado de tratamiento;

l) Exigir al Encargado del tratamiento, en todo momento, el respeto a las condiciones de seguridad y debido tratamiento de los datos;

m) Designar, en caso de corresponder, un Delegado de Protección de Datos. En caso de no corresponder, se debe establecer una persona o

área que asuma dicha función, quien dará trámite a las solicitudes de las personas Titulares de los datos.

Si el tratamiento de datos consiste en una cesión, el Responsable de tratamiento a quien se ceden los datos personales queda sujeto a las mismas obligaciones legales y reglamentarias que el cedente. Ambos son responsables.

En cualquier caso, pueden ser eximidos total o parcialmente de responsabilidad si demuestran que no se les puede imputar el hecho que ha producido el daño, correspondiendo a los mismos la carga de la prueba.

ARTÍCULO 37.- Deberes del Encargado de tratamiento. Los Encargados de tratamiento deben cumplir con los siguientes deberes:

a) Formalizar mediante un contrato escrito la prestación de servicios de tratamiento de datos por cuenta del Responsable de tratamiento. No requiere del consentimiento de la persona Titular de los datos;

b) Limitarse a llevar a cabo sólo aquellos tratamientos de datos encomendados por el Responsable de tratamiento;

c) Aplicar o utilizar los datos personales objeto de tratamiento con el fin que figure en el contrato, los que sólo pueden cederse con autorización expresa del Responsable de tratamiento;

d) Devolver una vez cumplida la prestación contractual, los datos personales tratados al Responsable de tratamiento o destruidos. El Responsable de Tratamiento puede autorizar una conservación por un máximo de DOS (2) años en caso que pueda presumir la posibilidad de ulteriores encargos;

e) Permitir al Responsable de tratamiento o Autoridad de Aplicación realizar inspecciones o auditorías para verificar el cumplimiento de la Ley y de lo pactado en el contrato de prestación de servicios;

f) Implementar medidas apropiadas, útiles, oportunas, pertinentes y eficaces para garantizar y poder demostrar el adecuado cumplimiento de la presente Ley y sus normas reglamentarias.

g) Tratar los datos personales bajo condiciones de seguridad apropiadas para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

h) Cumplir las instrucciones, órdenes o requerimientos que imparta la Autoridad de Aplicación;

i) Tramitar las solicitudes presentadas por la persona Titular de los datos, notificando al Responsable de tratamiento y dando aviso a la persona Titular de los datos de dicha notificación;

j) Informar en el plazo de ley a la Autoridad de Aplicación y al Responsable de tratamiento cuando se presenten incidentes de seguridad;

k) Designar, en caso de corresponder, un Delegado de Protección de Datos. En caso de no corresponder, se debe establecer una persona o área que asuma dicha función, quien dará trámite a las solicitudes de las personas Titulares de los datos.

El Encargado de tratamiento puede suscribir un contrato para subcontratar servicios que impliquen el tratamiento de datos solo cuando exista una autorización expresa del Responsable de tratamiento. En

estos casos el subcontratado asume el carácter de Encargado de tratamiento en los términos y condiciones previstos en esta Ley.

Si el subcontratado incumple sus obligaciones y responsabilidades, asume la calidad de Responsable de tratamiento en los términos y condiciones previstos en la presente Ley. Los contratos deben estipular el objeto, alcance, contenido, duración, naturaleza y finalidad del tratamiento de datos, el tipo de datos personales, las categorías de los datos, el cumplimiento del deber de confidencialidad y demás obligaciones y responsabilidades.

ARTÍCULO 38.- Política de tratamiento de datos personales. Los Responsables y los Encargados de tratamiento deben desarrollar sus políticas para el tratamiento de los datos personales, las que deberán instrumentarse a través de los medios más idóneos disponibles para informar en un lenguaje claro y sencillo a la persona Titular de datos como mínimo, la información detallada en el artículo 16 y su fecha de entrada en vigencia.

Cuando se realicen cambios sustanciales en el contenido de las mismas y la base legal para el tratamiento sea el consentimiento, los Responsables y Encargados de tratamiento deben notificar y obtener una nueva autorización por parte de la persona Titular de los datos.

ARTÍCULO 39.- Medidas para el cumplimiento de la responsabilidad proactiva. Las medidas adoptadas deben ser útiles, pertinentes, efectivas y proporcionales a las modalidades y finalidades del tratamiento de datos, su contexto, el tipo y categoría de datos tratados, y el riesgo que el referido tratamiento pueda acarrear sobre los derechos de la persona Titular de los datos.

Deben contemplar, como mínimo:

a) La adopción de procesos internos para llevar adelante de manera efectiva las medidas de responsabilidad;

b) La implementación de procedimientos ágiles y sencillos a efectos del ejercicio de los derechos por parte de las personas Titulares de los datos;

c) La realización de supervisiones o auditorías, internas o externas, para controlar el cumplimiento de las medidas adoptadas;

d) La implementación de procedimientos de evaluación de impacto;
Las medidas deben quedar documentadas y a disposición de la Autoridad de Aplicación en caso de ser requeridas.

ARTÍCULO 40. - Protección de datos desde el diseño y por defecto. La Protección de Datos desde el Diseño y por Defecto, se refiere a la integración de medidas de privacidad y seguridad en todas las etapas del ciclo de vida de los datos.

El Responsable de tratamiento debe, desde el diseño y antes del tratamiento, prever y aplicar medidas tecnológicas y organizativas apropiadas teniendo en cuenta el estado de la tecnología, los costos de la implementación y la naturaleza, ámbito, contexto y fines del tratamiento de los datos, así como los riesgos que entraña el tratamiento para garantizar los derechos a la protección de los datos de sus titulares.

Además debe aplicar las medidas con miras a garantizar que, por defecto, solo sean objeto de tratamiento aquellos datos personales que sean necesarios para cada uno de los fines del tratamiento.

Esta obligación se aplica a la cantidad, calidad y categoría de datos personales tratados, al alcance de su tratamiento, a su plazo de conservación y a su accesibilidad.

ARTÍCULO 41.- Evaluación de impacto relativa a la protección de datos personales. Si el Responsable de tratamiento 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 las personas Titulares de los datos, deberá realizar, de manera previa a la implementación, una evaluación del impacto relativa a la protección de los datos personales.

Sin perjuicio de ello, es obligatoria su realización en los siguientes casos:

a) Evaluación sistemática y exhaustiva de aspectos personales de personas humanas que se base en un tratamiento de datos automatizado y semiautomatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas humanas o que las afecten significativamente;

b) Tratamiento de datos sensibles a gran escala, o de datos relativos a antecedentes penales y contravencionales;

c) Observación sistemática a gran escala de una zona de acceso público.

La Autoridad de Aplicación podrá establecer otros casos obligatorios.

ARTÍCULO 42.- Contenido de la evaluación de impacto. La evaluación debe incluir, como mínimo:

a) Una descripción sistemática de las operaciones de tratamiento de datos previstas y de los fines del tratamiento, incluyendo, cuando proceda, el interés legítimo perseguido por el Responsable de tratamiento;

b) Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento de datos con respecto a su finalidad;

c) Una evaluación de los riesgos para la protección de los datos personales de las personas Titulares de los datos

d) Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de los datos personales.

ARTÍCULO 43.- Deber de informar. Cuando el resultado de la evaluación de impacto evidencie que el tratamiento entraña un alto riesgo, el Responsable de tratamiento debe informar de esta circunstancia a la Autoridad de Aplicación.

El informe debe incluir, como mínimo:

a) Las obligaciones respectivas del Responsable y Encargado de tratamiento, en particular en caso de tratamiento de datos dentro de un mismo Grupo económico;

b) Los fines y medios del tratamiento previsto;

c) Las medidas y garantías establecidas para minimizar los riesgos identificados y proteger los derechos de las personas Titulares de los datos;

d) En su caso, los datos de contacto del Delegado de Protección de Datos;

e) El resultado de la evaluación de impacto relativa a la protección de datos;

f) Cualquier otra información que solicite la Autoridad de Aplicación.

El Responsable de tratamiento no podrá iniciar el tratamiento de datos hasta tanto la Autoridad de Aplicación se pronuncie.

ARTÍCULO 44.- Delegado de Protección de Datos. Los Responsables y Encargados de tratamiento deben designar un Delegado de Protección de Datos en los siguientes supuestos:

a) Cuando se trate de una autoridad u organismo público;

b) Cuando las actividades del Responsable o Encargado de tratamiento de datos personales requieran un control permanente y sistematizado por su volumen, naturaleza, alcance o finalidades.

En el caso en que se trate de una autoridad u organismo público con dependencias subordinadas, se puede designar un único Delegado de Protección de Datos, teniendo en consideración su estructura organizativa.

Un Grupo económico puede nombrar un único Delegado de Protección de Datos siempre que esté en contacto permanente con cada una de las empresas que lo componen.

La designación como Delegado de Protección de Datos debe recaer en una persona que reúna los requisitos de idoneidad, capacidad y

conocimientos específicos para el ejercicio de sus funciones y puede ser desempeñado por un empleado del Responsable o Encargado de tratamiento o en el marco de un contrato de prestación de servicios, en tanto no haya conflicto de intereses.

El Delegado de Protección de Datos debe ejercer sus funciones de manera autónoma y libre de interferencias, sin recibir instrucciones y el Responsable o Encargado de tratamiento debe facilitarle los recursos.

No puede ser destituido ni sancionado por desempeñar sus funciones.

Cuando no sea obligatoria la designación, podrá designarse un Delegado de Protección de Datos de manera voluntaria.

ARTÍCULO 45.- Funciones del Delegado de Protección de Datos. El Delegado de Protección de Datos tiene las siguientes funciones:

a) Informar y asesorar a los Responsables y Encargados de tratamiento, así como a sus empleados, de las obligaciones a su cargo;

b) Promover y participar en el diseño y aplicación de una política de tratamiento de datos personales;

c) Supervisar el cumplimiento de la presente Ley y de la política de protección de datos;

d) Asignar responsabilidades, concientizar, formar al personal y realizar las auditorías correspondientes;

e) Ofrecer el asesoramiento que se le solicite para hacer una evaluación de impacto relativa a la protección de datos, cuando entrañe

un alto riesgo de afectación para los derechos de las personas Titulares de los datos, y supervisar luego su aplicación;

f) Cooperar y actuar como referente ante la Autoridad de Aplicación para cualquier consulta sobre el tratamiento de datos efectuado por el Responsable o Encargado de tratamiento.

ARTÍCULO 46.- Representantes de Responsables y Encargados de tratamiento. Cuando el Responsable o el Encargado de tratamiento no se encuentren establecidos en la REPÚBLICA ARGENTINA, deberán designar un Representante en el territorio nacional.

El Representante debe actuar en nombre del Responsable o del Encargado de tratamiento, y responderá los pedidos y solicitudes de la Autoridad de Aplicación y de las personas Titulares de los datos.

En caso de incumplimientos por parte del Responsable o del Encargado de tratamiento el Representante puede ser objeto de un proceso sancionatorio y pasible de las sanciones que se impongan.

El presente artículo no será aplicable cuando:

a) El tratamiento sea ocasional;

b) Se trate de organismos públicos extranjeros.

ARTÍCULO 47.- Registro. Créase el REGISTRO NACIONAL PARA LA PROTECCIÓN DE LOS DATOS PERSONALES. Deberán inscribirse obligatoriamente en el mismo:

a) Los Responsables y Encargados de tratamiento que deban tener un Delegado de Protección de Datos.

b) Los Responsables y Encargados de tratamiento de datos que deban contar con un Representante en la REPÚBLICA ARGENTINA.

La Autoridad de Aplicación tendrá a su cargo el dictado de la normativa complementaria del registro que se crea por este artículo.

ARTÍCULO 48.- Mecanismos de regulación vinculantes. La Autoridad de Aplicación promoverá la elaboración de mecanismos de regulación vinculantes que tengan por objetivo contribuir a la correcta aplicación de la presente Ley, teniendo en cuenta las características específicas del tratamiento de datos que se realice, así como el efectivo ejercicio y respeto de los derechos de la persona Titular de los datos.

Tales mecanismos pueden consistir, entre otros, en códigos de ética, de buenas prácticas, normas corporativas vinculantes, sellos de confianza, certificaciones u otros mecanismos que coadyuven a contribuir con el objetivo señalado.

Los Responsables o Encargados de tratamiento pueden adherirse a ello de manera voluntaria.

Las asociaciones u otras entidades representativas de categorías de Responsables o Encargados de tratamiento pueden adoptar mecanismos de regulación vinculantes que resulten obligatorios para todos sus miembros. Estos deben ser presentados para la homologación de la Autoridad de Aplicación, la cual determinará si se adecúan a las disposiciones de esta Ley y, en su caso, los aprobará o indicará las correcciones que estime necesarias.

Los que resulten aprobados serán registrados y dados a publicidad por la Autoridad de Aplicación.

CAPÍTULO VI

PROTECCIÓN DE DATOS DE INFORMACIÓN CREDITICIA

ARTÍCULO 49.- Protección de datos de información crediticia del sector financiero y no financiero. En la prestación de servicios de información crediticia sólo pueden tratarse datos personales de carácter patrimonial relativos a la solvencia económica y al crédito cuando se cuente con una base legal conforme a lo establecido en el artículo 13 de la presente Ley.

Se prohíbe a las empresas prestadoras de servicios de información crediticia el tratamiento de datos de los ascendientes y descendientes hasta el segundo grado y cónyuge de la persona Titular de los datos, exceptuando el supuesto de quienes participen dentro de una misma sociedad comercial.

No se pueden tratar los datos comerciales negativos referidos a la prestación de los servicios públicos esenciales.

ARTÍCULO 50.- Plazo de conservación de la información crediticia. En la prestación de servicios de información crediticia sólo se pueden tratar datos personales que sean significativos para evaluar la solvencia económico financiera durante los últimos CINCO (5) años. El plazo se reduce a DOS (2) años si el deudor cancela o extingue la obligación, a contar a partir de la fecha precisa en que lo ha hecho, y esto debe constar en el informe crediticio.

ARTÍCULO 51.- Deber de comunicación. A solicitud de la persona Titular de los datos, los Responsables de tratamiento que elaboren un sistema de puntuación y/o calificación de acuerdo al comportamiento crediticio de las personas deberán comunicarle el detalle de la fórmula aplicada, las variables consideradas, el procedimiento y la información que se

toma en cuenta, o el algoritmo que se utiliza, y su composición y las consecuencias de su aplicación.

Las entidades comprendidas dentro de la Ley N° 21.526 de Entidades Financieras y aquellas personas y entidades públicas y privadas no financieras, cuando a juicio del BANCO CENTRAL DE LA REPÚBLICA ARGENTINA lo aconseje el volúmen de sus operaciones y razones de política monetaria y crediticia, deben comunicar en forma diligente a la persona Titular de los datos el cambio de situación crediticia, por un medio que permita acreditar el envío y su fecha.

Dicha comunicación se debe efectuar, cuando las obligaciones pasen de cumplimiento normal a incumplimiento, dentro de los DIEZ (10) días hábiles de producida la nueva clasificación. El cedente tiene la carga de acreditar el cumplimiento de la comunicación aquí dispuesta.

En el caso que se deniegue a la persona Titular de los datos la celebración de un contrato, solicitud de trabajo, servicio, crédito comercial o financiero, sustentado en un informe crediticio, se le debe informar tal circunstancia.

ARTÍCULO 52.- Publicación de la información crediticia. El BANCO CENTRAL DE LA REPÚBLICA ARGENTINA publicará en el marco de sus competencias la información cedida por las entidades crediticias relativas al cumplimiento o incumplimiento de obligaciones de contenido patrimonial de manera amplia y transparente.

En el caso de los archivos o bases de datos públicas del BANCO CENTRAL DE LA REPÚBLICA ARGENTINA conformadas por cesión de información suministrada por entidades crediticias, los derechos de rectificación, oposición, supresión y portabilidad deben ejercerse ante la entidad cedente del dato impugnado.

Asimismo, si el reclamo se relaciona con una información incorrecta en bases de datos de información crediticia difundida por prestadoras de servicios de información crediticia se debe dirigir directamente a ellas.

Toda modificación debe ser comunicada al BANCO CENTRAL DE LA REPÚBLICA ARGENTINA, quien efectuará la actualización de sus bases de datos en un tiempo razonable atendiendo a sus capacidades operativas.

CAPÍTULO VII

AUTORIDAD DE APLICACIÓN

ARTÍCULO 53.- Autoridad de Aplicación. La Autoridad de Aplicación de la presente Ley es la AGENCIA DE PROTECCIÓN DE LOS DATOS PERSONALES.

Gozará de autonomía funcional y autarquía financiera y actuará como organismo descentralizado en la jurisdicción del Ministerio de Justicia de la Nación o en la que en un futuro lo reemplace.

Tendrá su domicilio en la Capital de la REPÚBLICA ARGENTINA y podrá establecer agencias regionales en el resto del país.

Estará dirigida y administrada por un Director Ejecutivo designado por el PODER EJECUTIVO con acuerdo del SENADO; durará CUATRO (4) años en sus funciones pudiendo ser designado nuevamente por única vez. El Poder Ejecutivo Nacional podrá realizar nombramientos en comisión durante el tiempo que insuma el otorgamiento del acuerdo del Senado de la Nación.

Para ser designado Director Ejecutivo, deberá poseer título universitario de grado, preferentemente en Derecho y Ciencias Informáticas y antecedentes técnicos y profesionales en la materia.

El Director Ejecutivo tendrá dedicación exclusiva en su función, y percibirá una remuneración equivalente a la de un Juez de Primera Instancia, encontrándose alcanzado por las incompatibilidades fijadas por ley para los funcionarios públicos y podrá ser removido por el PODER EJECUTIVO por mal desempeño de sus funciones, grave negligencia, por la comisión de delitos dolosos de cualquier especie o por inhabilidad física o moral sobreviniente a su incorporación.

ARTÍCULO 54.- Funciones y atribuciones de la Autoridad de Aplicación. La Autoridad de Aplicación tendrá las siguientes funciones y atribuciones:

a) Dictar las normas complementarias y criterios orientadores que se deben observar para la aplicación de la presente Ley;

b) Ejercer la supervisión, control y evaluación de las actividades efectuadas por el Responsable y Encargado de tratamiento de datos personales. En caso de corresponder podrá requerir el auxilio de la fuerza pública y solicitar autorización judicial para allanar;

c) Tramitar los requerimientos y denuncias interpuestos en relación con el tratamiento de datos, garantizando la tutela administrativa efectiva;

d) Solicitar información a los Responsables o Encargados de tratamiento, Delegados de Protección de Datos y Representantes, los que deberán proporcionar lo que se les requiera. La Autoridad de Aplicación deberá garantizar la seguridad y confidencialidad de la información y elementos suministrados;

e) Dictar órdenes, comunicaciones, y otros actos administrativos para garantizar el debido tratamiento de los datos personales y aplicar las sanciones por violación de esta Ley y de las Reglamentaciones;

f) Iniciar las actuaciones administrativas de oficio; a petición de parte; o por solicitud de otra autoridad, de un tercero o de asociaciones u organizaciones con interés legítimo;

g) Implementar mecanismos voluntarios de solución de controversias para que las personas Titulares de los datos y los Responsables o Encargados de tratamiento lleguen a acuerdos que garanticen el debido tratamiento de los datos personales y los derechos de las personas titulares;

h)Constituirse en querellante en las acciones penales que correspondan;

i) Interponer acciones colectivas de habeas data conforme a lo establecido en esta Ley;

j) Aprobar las cláusulas contractuales modelo para la transferencia internacional de datos;

k) Homologar los mecanismos de regulación vinculantes y supervisar su cumplimiento;

l) Crear, regular y aprobar los mecanismos de certificación en materia de protección de datos y los requisitos que deben cumplir los organismos de certificación;

m) Promover acciones de cooperación y armonización normativa con autoridades de protección de datos personales de otros países,

entidades u organismos internacionales, y Estados subnacionales; y celebrar convenios de cooperación y contratos con organizaciones públicas o privadas, nacionales o extranjeras, en el ámbito de su competencia, para el cumplimiento de sus funciones;

n) Asistir, asesorar y capacitar a las personas y entidades, públicas y privadas, acerca de los alcances de la presente Ley;

o) Promover y difundir los derechos a la privacidad, el debido tratamiento de datos y la autodeterminación informativa, así como una gestión responsable, ética y transparente de los procesamientos automatizados o semiautomatizados;

p) Desarrollar investigación aplicada y conocimiento sobre la protección de datos personales;

q) Promover, organizar y desarrollar programas tendientes a la protección de datos personales de niños, niñas y adolescentes, preferentemente en internet, juegos electrónicos y otras plataformas digitales;

r) Generar estrategias para la prevención de la violencia digital en relación con la defensa de la privacidad y tratamiento de datos;

s) Promover la incorporación de contenidos educativos vinculados al tratamiento de datos, la privacidad y la autodeterminación informativa e implementar campañas pedagógicas de difusión;

t) Promover la capacitación y formación profesional en materia de protección de datos personales;

u) Ejercer otras facultades que le sean asignadas por la Ley o su Reglamentación.

CAPÍTULO VIII

PROCEDIMIENTOS Y SANCIONES

ARTÍCULO 55.- Procedimientos. A los efectos de constatar el cumplimiento de las disposiciones de la presente Ley, la Autoridad de Aplicación podrá iniciar procedimientos:

a) A instancia de la persona Titular de los datos;

b) A instancia de otra autoridad, un tercero, asociaciones u organizaciones, siempre que exista un interés legítimo, por denuncia de violaciones a la presente Ley;

c) De oficio.

Para el caso del procedimiento previsto en el a) será de aplicación lo establecido en la presente y de manera supletoria la Ley Nacional de Procedimientos Administrativos Nº 19.549 y sus modificatorias. En los procedimientos contemplados en los incisos b) y c) se aplicará la Ley 19.549 citada.

ARTÍCULO 56.- Trámite de protección de los datos personales. El Titular de los datos o su representante legal pueden realizar una denuncia, en forma gratuita, mediante cualquier medio habilitado para dicho efecto por la Autoridad de Aplicación, expresando con claridad el contenido de su requerimiento y los preceptos de esta Ley que considere vulnerados, acreditando haber efectuado la intimación prevista en el artículo 34 de esta Ley.

Dicha denuncia debe realizarse dentro de los TREINTA (30) días hábiles siguientes a la fecha en que se le haya comunicado la respuesta o en cualquier momento si se venció el plazo y no hubiera obtenido respuesta.

La Autoridad de Aplicación, dentro de los DIEZ (10) días hábiles de presentada la denuncia, intimará a los Responsables o Encargados de tratamiento para que en el plazo de DIEZ (10) días hábiles emitan respuesta, ofrezcan las pruebas que estimen pertinente y manifiesten por escrito lo que a su derecho convenga. Dicho plazo, podrá prorrogarse por el mismo término y por única vez, a solicitud debidamente fundada y previa al vencimiento.

En caso de tener que producir prueba, la Autoridad de Aplicación determinará el plazo según la complejidad de la misma, el cual nunca podrá exceder de TREINTA (30) días hábiles. Y quedará el trámite en condiciones de dictar Resolución.

ARTÍCULO 57.- Resolución. La Autoridad de Aplicación podrá, mediante resolución fundada:

a) Desestimar las denuncias presentadas;

b) En caso de considerar que asiste derecho a la persona Titular de los datos, requerir al Responsable o Encargado de tratamiento que haga efectivo el ejercicio de los derechos objeto de protección, debiendo dar cuenta por escrito de dicho cumplimiento a la Autoridad de Aplicación dentro de los QUINCE (15) días hábiles de efectuado;

c) En caso de verificarse incumplimientos a la presente Ley, aplicar las sanciones previstas en el artículo 61 de la presente Ley.

La Autoridad de Aplicación dictará la resolución dentro de un plazo que no podrá exceder de TREINTA (30) días hábiles.

ARTÍCULO 58.- Notificaciones. Son válidas las notificaciones realizadas por medios electrónicos conforme la normativa que dicte la Autoridad de Aplicación, teniendo en consideración el principio de neutralidad tecnológica.

ARTÍCULO 59.- Recurso de Reconsideración y agotamiento de la vía. Contra las resoluciones emitidas por la Autoridad de Aplicación en los procedimientos contemplados en el artículo 55 de esta Ley puede interponerse el recurso de reconsideración previsto en el artículo 84 del Reglamento de Procedimientos Administrativos aprobado por Decreto N° 1759/72 y sus modificatorios.

Dicha resolución agota la vía administrativa.

No procede el recurso de alzada.

ARTÍCULO 60.- Medidas correctivas. En caso de incumplimiento de las disposiciones previstas en la presente Ley, su Reglamentación y normas complementarias, la Autoridad de Aplicación puede dictar medidas correctivas con el objeto de evitar la continuidad o la reincidencia en la conducta infractora, sin perjuicio de la aplicación de las correspondientes sanciones administrativas.

ARTÍCULO 61.- Sanciones. La Autoridad de Aplicación puede aplicar a los Responsables y Encargados de tratamiento, y a sus representantes, las siguientes sanciones:

a) Apercibimientos;

b) Multas;

c) Suspensión de las actividades relacionadas con el tratamiento de datos personales;

d) Cierre temporal de las operaciones;

e) Cierre definitivo de las operaciones.
La Autoridad de Aplicación debe dar a publicidad la resolución en su sitio web y, si lo considera pertinente, en el BOLETÍN OFICIAL, y ordenar su publicación en el sitio web del Responsable de tratamiento, a costa de este último.

La Autoridad de Aplicación se encuentra facultada para dictar las normas complementarias y/o aclaratorias a tales fines.
La Reglamentación determinará, garantizando el principio del debido proceso en el marco de la tutela administrativa efectiva, las condiciones y procedimientos para la aplicación de las sanciones previstas.

ARTÍCULO 62.- Determinación de la unidad móvil. La Autoridad de Aplicación podrá aplicar multas sobre la base de la unidad móvil definida en la presente Ley.

El valor inicial de la unidad móvil se establece en CINCUENTA MIL ($ 50.000), y debe ser actualizado anualmente conforme a la variación del Índice de Precios al Consumidor (IPC) que publica el INSTITUTO NACIONAL DE ESTADÍSTICA Y CENSOS (INDEC) o el indicador oficial que lo pudiera reemplazar en el futuro.

La Autoridad de Aplicación realizará la actualización de la unidad móvil el último día hábil de cada año, entrando en vigencia el valor actualizado desde el momento de su publicación en el BOLETÍN OFICIAL.

ARTÍCULO 63.- Multas. Las multas se pueden establecer desde las CINCO (5) unidades móviles, hasta UN MILLÓN (1.000.000) de unidades móviles; o desde el DOS POR CIENTO (2 %), hasta el CINCO POR CIENTO (5 %) de la facturación total anual global del infractor en el ejercicio financiero anterior a la aplicación de la sanción.

La Autoridad de Aplicación determinará los topes de las multas aplicables en cada caso.

ARTÍCULO 64.- Incumplimiento por parte del Sector Público. En caso de que la Autoridad de Aplicación advierta un presunto incumplimiento de las disposiciones de la presente Ley por parte de un organismo del Sector Público, puede imponer medidas correctivas con el fin de subsanar y mitigar los efectos producidos por el incumplimiento de la presente Ley.

Asimismo podrá aplicar las sanciones previstas en el artículo 61, con excepción de las multas, sin perjuicio de las responsabilidades disciplinarias, civiles y penales que correspondan.

ARTÍCULO 65.- Graduación. Las sanciones a las que se refiere el artículo 61 de la presente Ley deben ser graduadas, en leves, graves y gravísimas, con atención a los siguientes criterios:

a) La naturaleza y dimensión del daño o peligro a los intereses jurídicos tutelados por la presente Ley;

b) El beneficio económico obtenido por el infractor o terceros, en virtud de la comisión de la infracción;

c) La reincidencia en la comisión de la infracción;

d) La resistencia, negativa u obstrucción a la acción investigadora o de vigilancia de la Autoridad de Aplicación;

e) El incumplimiento de los requerimientos u órdenes impartidas por la Autoridad de Aplicación;

f) El reconocimiento o aceptación expresa que haga el investigado sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar;

g) La condición económica del infractor;

h) La adopción demostrada de medidas correctivas y mecanismos y procedimientos internos tendientes al tratamiento seguro y adecuado de los datos y capaces de minimizar el daño;

i) La adopción de mecanismos de regulación vinculantes;

j) La proporcionalidad entre la gravedad de la falta y de la sanción;

k) La designación voluntaria de un Delegado de Protección de Datos;

l) La notificación oportuna de incidentes de seguridad;

CAPÍTULO IX

ACCIÓN DE HABEAS DATA

ARTÍCULO 66.- Procedencia. La acción de habeas data procede para tutelar los derechos que resulten restringidos, alterados, lesionados o amenazados por un tratamiento de datos personales contrario a la

normativa vigente por parte de Responsables o Encargados de tratamiento.

ARTÍCULO 67.- Legitimación activa y pasiva. La acción de habeas data podrá ser ejercida por el Titular de los datos afectados o su representante legal.

En el caso de las personas fallecidas, la acción podrá ser ejercida por sus sucesores universales.

En el proceso podrá intervenir, en forma coadyuvante y cuando corresponda, la Autoridad de Aplicación, quien deberá ser notificada del inicio de la acción por parte del Juez interviniente.

La acción de habeas data podrá ser entablada en representación colectiva por la Autoridad de Aplicación, el DEFENSOR DEL PUEBLO o las asociaciones u organizaciones con interés legítimo, siempre que su objeto se limite a la impugnación de tratamientos que conllevan violaciones generalizadas o afectaciones a intereses individuales homogéneos del colectivo que dicen representar.

En tal caso, no podrán tener acceso a los datos de las demás personas que integran el colectivo por ellas representado, sino solo a los datos propios.

La acción procede respecto de los Responsables y Encargados de tratamiento.

De manera excepcional, los Responsables o Encargados de tratamiento, podrán interponer la acción de habeas data contra otros Responsables o Encargados de tratamiento cuando el incumplimiento

de sus obligaciones legales o convencionales, pueda generarles un perjuicio.

ARTÍCULO 68.- Competencia. Es competente para entender en la acción de habeas data el juez del domicilio del accionante, del requerido o del lugar donde se firmó el acuerdo para el tratamiento de datos, a elección del accionante.

Procede la competencia federal cuando:

a. La acción se interponga en contra de los Responsables y Encargados de tratamiento que integren el Sector Público Nacional;

b. Las bases de datos se encuentren interconectadas en redes interjurisdiccionales, nacionales o internacionales.

ARTÍCULO 69.- Procedimiento aplicable. La acción de habeas data tramita según las disposiciones de la presente Ley, y de manera supletoria se aplicará el procedimiento que corresponda a la acción de amparo y en su caso, las normas del Código Procesal Civil y Comercial de la Nación, 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, incluso la de recalificar la vía procesal utilizada.

ARTÍCULO 70.- Requisitos de interposición. Debe interponerse por escrito, individualizando con la mayor precisión posible el nombre y domicilio del Responsable o Encargado de tratamiento y, en su caso, el nombre de la base de datos o cualquier otra información que pudiera ser útil a efectos de identificarla.

Cuando la acción se interponga en contra del tratamiento de datos efectuado por el Sector Público Nacional, se debe procurar establecer la autoridad u organismo público del cual dependiera el Responsable o el Encargado de tratamiento.

El accionante deberá alegar las razones por las cuales considera que se está efectuando un tratamiento de sus datos personales y los motivos por los cuales considera que procede el ejercicio de la acción de habeas data y los derechos que entiende le corresponden o le han sido conculcados.

El accionante podrá solicitar al Juez que, mientras dure el procedimiento, el Responsable o el Encargado de tratamiento informe que los datos cuestionados están sometidos a un proceso judicial.

El Juez podrá disponer el bloqueo provisional del acceso a los datos personales objeto del juicio, cuando sea manifiesto el carácter ilícito de su tratamiento o ellos sean inequívocamente falsos o inexactos.

ARTÍCULO 71.- Trámite. Declarada admisible la acción, el Juez requerirá al Responsable o Encargado de tratamiento un informe circunstanciado concerniente a la información del accionante.

El requerido deberá cumplir la carga de ofrecer prueba en oportunidad de contestar el informe.

La omisión del pedido de informe es causa de nulidad del proceso.

También puede requerir informes sobre el soporte técnico de datos, documentación de base relativa al tratamiento y cualquier otro aspecto que resulte conducente a la resolución de la causa que estime procedente.

El plazo para contestar el informe no puede ser mayor a CINCO (5) días hábiles.

De manera excepcional el Juez podrá ampliar el plazo a solicitud debidamente fundada del requerido.

Los Responsables o Encargados de tratamiento no pueden alegar la confidencialidad de la información que se les requiera, salvo el caso en que se afecten las fuentes de información periodística.

Si un Responsable o Encargado de tratamiento se opone a la remisión del informe solicitado, con invocación de las excepciones autorizadas por la presente Ley o por una ley específica, debe acreditar los extremos que hacen aplicable la excepción legal. En tales casos, el Juez podrá tomar conocimiento personal y directo de la información requerida manteniendo su confidencialidad.

ARTÍCULO 72.- Contestación del informe. Al contestar el informe, el requerido deberá expresar las razones por las cuales efectuó el tratamiento cuestionado y, en su caso, los motivos por los que no evacuó el pedido efectuado por el accionante.

ARTÍCULO 73.- Ampliación. Contestado el informe, el accionante puede, en el término de TRES (3) días hábiles, ampliar el objeto y ofrecer, en el mismo acto, la prueba pertinente. De esta presentación se debe dar traslado al requerido por igual término para que conteste y ofrezca prueba.

ARTÍCULO 74.- Sentencia. Vencido el plazo para la contestación del informe o contestado este, o luego de contestada la ampliación, y, en su caso, producida la prueba, se dictará sentencia, en un plazo máximo CINCO (5) días hábiles.

De estimarse procedente, se ordenará las acciones correspondientes conforme peticionado por el accionante, estableciendo un plazo para su cumplimiento.

Asimismo, deberá ser comunicada a la Autoridad de Aplicación.

Sólo serán apelables la sentencia que declara la inadmisibilidad y la sentencia definitiva.

El recurso deberá interponerse dentro de los TRES (3) días hábiles de notificada la resolución impugnada y será fundado, debiendo denegarse o concederse en ambos efectos dentro de los TRES (3) días hábiles. En este último caso se elevará el expediente al respectivo Tribunal de Alzada dentro de UN (1) día hábil de ser concedido.

En caso de que fuera denegado, entenderá dicho Tribunal en el recurso directo que deberá articularse dentro de los TRES (3) días hábiles de ser notificada la denegatoria, debiendo dictarse sentencia dentro de los TRES (3) días hábiles.

CAPÍTULO X

DISPOSICIONES COMPLEMENTARIAS

ARTÍCULO 75.- Las normas de la presente Ley son de orden público y de aplicación en todo el territorio nacional, con excepción de las normas procesales del CAPÍTULO 9 que se regirán por lo establecido en los respectivos ordenamientos procesales provinciales.

Se invita a las Provincias y a la Ciudad Autónoma de Buenos Aires a adherir a las normas de esta Ley que fueren de aplicación exclusiva en jurisdicción nacional.

ARTÍCULO 76.- Sustitúyese el artículo 19 de la Ley N° 27.275 y su modificatorio, el que quedará redactado de la siguiente manera:

“*ARTÍCULO 19.-AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA. Créase la AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA, como ente autárquico que funcionará con autonomía funcional en el ámbito de la JEFATURA DE GABINETE DE MINISTROS. La AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA debe velar por el cumplimiento de los principios y procedimientos establecidos en la presente ley, garantizar el efectivo ejercicio del derecho de acceso a la información pública y promover medidas de transparencia activa*.”

ARTÍCULO 77.- Sustitúyese el artículo 24 de la Ley N° 27.275 y su modificatorio, el que quedará redactado de la siguiente manera:

“*ARTÍCULO 24. - Son competencias y funciones de la Agencia de Acceso a la Información Pública:*

a) Elaborar y proponer para su aprobación, el diseño de su estructura orgánica, y designar a su planta de agentes, conforme a la normativa vigente en materia de designaciones en el ámbito de la ADMINISTRACIÓN PÚBLICA NACIONAL;

b) Preparar su presupuesto anual;

c) Redactar y aprobar el Reglamento de Acceso a la Información Pública aplicable a todos los sujetos obligados;

d) Implementar una plataforma tecnológica para la gestión de las solicitudes de información y sus correspondientes respuestas;

e) Requerir a los sujetos obligados que modifiquen o adecuen su organización, procedimientos, sistemas de atención al público y recepción de correspondencia a la normativa aplicable a los fines de cumplir con el objeto de la presente ley;

f) Proveer un canal de comunicación con la ciudadanía con el objeto de prestar asesoramiento sobre las solicitudes de información pública y, en particular, colaborando en el direccionamiento del pedido y refinamiento de la búsqueda;

g) Coordinar el trabajo de los responsables de acceso a la información pública designados por cada uno de los sujetos obligados, en los términos de lo previsto en el artículo 30 de la presente ley;

h) Elaborar y publicar estadísticas periódicas sobre requirentes, información pública solicitada, cantidad de denegatorias y cualquier otra cuestión que permita el control ciudadano a lo establecido por la presente ley;

i) Publicar periódicamente un índice y listado de la información pública frecuentemente requerida que permita atender consultas y solicitudes de información por vía de la página oficial de la red informática de la Agencia de Acceso a la Información Pública;

j) Publicar un informe anual de rendición de cuentas de gestión;

k) Elaborar criterios orientadores e indicadores de mejores prácticas destinados a los sujetos obligados;

l) Elaborar y presentar ante el Honorable Congreso de la Nación propuestas de reforma legislativa respecto de su área de competencia;

m) Solicitar a los sujetos obligados expedientes, informes, documentos, antecedentes y cualquier otro elemento necesario a los efectos de ejercer su labor;

n) Difundir las capacitaciones que se lleven a cabo con el objeto de conocer los alcances de la presente ley;

o) Recibir y resolver los reclamos administrativos que interpongan los solicitantes de información pública según lo establecido por la presente ley respecto de todos los obligados, con excepción de los previstos en los incisos b) al f) del artículo 7° de la presente, y publicar las resoluciones que se dicten en ese marco;

p) Promover las acciones judiciales que correspondan, para lo cual la Agencia de Acceso a la Información Pública tiene legitimación procesal activa en el marco de su competencia;

q) Impulsar las sanciones administrativas pertinentes ante las autoridades competentes correspondientes en los casos de incumplimiento a lo establecido en la presente ley;

r) Celebrar convenios de cooperación y contratos con organizaciones públicas o privadas, nacionales o extranjeras, en el ámbito de su competencia, para el cumplimiento de sus funciones;

s) Publicar los índices de información reservada elaborados por los sujetos obligados.”

CAPÍTULO XI

DISPOSICIONES TRANSITORIAS

ARTÍCULO 78 - Derogación. Deróganse las Leyes N° 25.326 y su modificatoria N° 26.343 una vez que entre en vigencia la presente ley.

ARTÍCULO 79.- Reglamentación. El Poder Ejecutivo dictará las normas complementarias, aclaratorias y operativas necesarias para la efectiva aplicación de lo dispuesto en la presente ley en el plazo de SESENTA (60) días corridos de su publicación.

ARTÍCULO 80 - Designación de la Autoridad de Aplicación. El Poder Ejecutivo dentro del plazo de SESENTA (60) días corridos de publicada la presente deberá designar la autoridad de aplicación y remitir al SENADO el pliego correspondiente y poner en funcionamiento su estructura.

ARTÍCULO 81 - Disposiciones presupuestarias. Autorizase al Jefe de Gabinete de Ministros a readecuar las partidas presupuestarias para la implementación de la presente ley.

Asimismo, deberá preverse en el presupuesto del año inmediato subsiguiente la incorporación de los recursos necesarios para el correcto cumplimiento de las funciones de la autoridad de aplicación.

ARTÍCULO 82.- Vigencia. La presente Ley entrará en vigencia transcurridos CIENTO OCHENTA (180) días corridos desde su publicación en el BOLETÍN OFICIAL. Excepto los artículos 79, 80 y 81, que comenzarán a regir a partir de la referida publicación.

ARTÍCULO 83.- Comuníquese al PODER EJECUTIVO.

Claudio M. Doñate

FUNDAMENTOS

Señora Presidente:

Ante el avance tecnológico del último decenio se ha impuesto la necesidad de crear un paraguas jurídico de protección a los datos personales para contar con una regulación que permita abordar los nuevos desafíos que se presentan.

Cada vez que interactuamos en la red, ya sea a través de una compra online, una red social o la suscripción a un newsletter, autorizamos la recolección de nuestros datos personales, sin entender acabadamente los términos y condiciones que aceptamos e incluso, muchas otras, ni siquiera manifestamos de manera expresa dicho consentimiento.

A esto, se suma el desarrollo de nuevas tecnologías y entre ellas la inteligencia artificial (IA), que ahora van más allá de analizar y clasificar datos, ya que, hasta crean nuevos contenidos. Con la IA se analizan y utilizan los datos recolectados de forma automatizada, para la elaboración de perfiles y la toma de decisiones.

En otros términos, cuando navegamos y utilizamos motores de búsqueda, producimos datos que van desde nuestros intereses, ubicación, gustos, e incluso el tiempo que tardamos leyendo o viendo algo específico; y estos datos son utilizados a través de algoritmos para inferir nuestras preferencias y orientar la publicidad, cuando no para incidir en nuestro comportamiento. Y esta capacidad de inferir datos,

genera una profunda preocupación por la afectación a las libertades, a la privacidad y a la seguridad de los datos personales.

Por todo esto, he presentado bajo el expte. S-2573/24, un proyecto de Ley de regulación integral de la inteligencia artificial y ahora de manera complementaria, la presente iniciativa pretende abordar y dar respuesta a estos nuevos desafíos que presentan los avances tecnológicos en la protección de nuestra intimidad y datos personales.

En Argentina, la intimidad, el honor y la dignidad humana detentan rango constitucional. Nuestra Constitución Nacional, consagra la inviolabilidad de la propiedad, el domicilio y la correspondencia privada sin orden escrita y fundada de autoridad pública y la protección de los datos personales a través del hábeas data.

Pero lamentablemente la normativa no se actualizó a la par de los avances tecnológicos, generando así nuevas formas de vulneraciones a nuestra privacidad y seguridad de datos personales. La única ley respecto a esa materia es la N° 25.326 y data del año 2000.

Es habitual, en los tiempos que corren, que la recolección de datos se produzca mediante un mero aviso o incluso, a través del mero uso de las aplicaciones, lo que ocasiona que los usuarios desconozcan qué datos autorizan a recolectar, para qué, quiénes y con qué fines. Y sin normativa acorde, decanta en un uso abusivo.

Las políticas de tratamiento de datos personales y sus actualizaciones en las diferentes apps no son comprendidas y a veces ni siquiera leídas por los usuarios al otorgar su consentimiento, el cual ha pasado a ser un mero formalismo, que, lejos está de garantizar el control sobre la información personal y su consiguiente protección. ¿Se puede consentir aquello que no se comprende?. La respuesta negativa se impone.

Conforme una encuesta realizada por Amnistía Internacional, en Argentina 3 de cada 4 personas están preocupadas por el uso de los datos personales que hacen las grandes compañías de tecnología. La encuesta, también reveló que, el 80% de los consultados considera que debe regularse[1].

Hay que desterrar la falsa dicotomía entre la innovación versus la regulación. Es necesario promover y promocionar la innovación tecnológica y el desarrollo de la economía del conocimiento y digital y, en paralelo, establecer reglas claras desde un enfoque de derechos humanos en consonancia con los estándares internacionales en la materia.

En este sentido, muchas han sido las iniciativas legislativas presentadas por diferentes espacios políticos, lo que indica la existencia de una coincidencia en la necesidad de actualización del marco regulatorio vigente y la vocación por la protección de datos personales.

De todos los proyectos destaca el Expte PE-108/23 enviado por el gobierno mandato cumplido 2019-2023, hoy caducado. Dicho proyecto fue el resultado de un arduo trabajo previo, que se dividió en diferentes etapas, tendientes a realizar un proceso participativo, incluso el origen del mismo se remonta a 2018.

Así, conforme se desprende de la página oficial: “*... la Agencia de Acceso a la Información Pública inició un proceso de debate participativo, abierto y transparente llevando adelante mesas preparatorias y mesas de diálogo con diversos sectores de la sociedad,*

[1] https://amnistia.org.ar/noticias/en-argentina-3-de-cada-4-personas-estan-preocupadas-por-el-uso-de-los-datos-personales-que-hacen-las-grandes-companias-de-tecnologia

durante los meses de julio y agosto. Producto de la participación y el debate, se redactó una Propuesta de Anteproyecto que fue presentada el pasado 30 de agosto, en la Cúpula del Centro Cultural Kirchner.

El 12 de septiembre se habilitó la instancia de consulta pública (Resolución AAIP 119/2022) con el propósito de garantizar la efectiva participación de la ciudadanía, de acuerdo con el Reglamento General para la Elaboración Participativa de Normas (Anexo V del Decreto 1172/03). Sin embargo, a raíz de la presentación de distintas solicitudes para extender el plazo de la participación, se prorrogó la consulta pública hasta el 11 de octubre inclusive (Resolución AAIP 145/2022). A lo largo de este proceso se recibieron 173 documentos con opiniones, aportes y comentarios presentados por 123 participantes correspondientes a la ciudadanía en general, organizaciones de la sociedad civil, universidades e investigadores, sector privado y sector público nacional e internacional. Como resultado de este proceso de debate, se presentó un Nuevo Proyecto de Ley de Protección de Datos Personales.”

Y sobre dicha base, que tomó como aporte conceptual los más recientes estándares, recomendaciones y lecciones aprendidas en nuestra región y en el mundo durante los últimos años, entre ellos la normativa de la Unión Europea, Brasil, Ecuador, Chile, Paraguay y Costa Rica, la iniciativa se sustenta en 3 pilares:

a) el derecho humano a la protección de los datos personales y la autodeterminación informativa,

b) la innovación tecnológica basada en principios éticos que promueva un desarrollo económico inclusivo y

c) la construcción de confianza a través de reglas de juego claras.

La presente iniciativa busca retomar lo planteado en el Expte PE-108/23, realizando algunas modificaciones producto del tiempo transcurrido y para adecuar al Expte S-2573/24 ya citado.

Entre los puntos destacables del proyecto, tenemos que se establece el principio de extraterritorialidad, que implica que la normativa se aplicará en distintos supuestos, aún cuando los Responsables de tratamiento de datos no se encuentren en territorio nacional.

También, el Principio de neutralidad tecnológica, es decir, se aplica a cualquier tratamiento de datos personales, con independencia de las técnicas, procesos o tecnologías, actuales o futuras que se utilicen.

Además, se instituyen los principios que se deben respetar para el adecuado tratamiento de los datos personales. Entre ellos, el principio de licitud, lealtad y transparencia; de finalidad; de minimización de datos; el de exactitud, integridad y confidencialidad; de preeminencia; de limitación del plazo de conservación y de responsabilidad proactiva y demostrada.

Este último principio implica que los responsables y otros sujetos que realizan tratamiento de datos deben adoptar las medidas oportunas y efectivas con el fin de garantizar un tratamiento adecuado y ser capaces de demostrar a la Autoridad de Aplicación su efectiva implementación. Además se encuentran obligados a la implementación de la debida diligencia en la materia.

Por otro lado, se determinan las bases legales para el tratamiento de datos. En este punto, es de destacar que hay un cambio de paradigma en relación con la ley vigente, y se abandona la lógica basada en la prohibición de tratamiento, en caso de no contar con el consentimiento del titular y se presentan supuestos que legitiman y dan base legal.

Igualmente, el consentimiento sigue siendo uno de los principios rectores para el tratamiento de datos personales. Por ello, se determinan sus características.

También, se regula el tratamiento de datos sensibles, el tratamiento de datos en el sector público y la protección especial de datos personales en el caso de niñas, niños y adolescentes.

Se incorporan reglas aplicables a todos aquellos que hacen tratamiento de datos, entre ellas la imposición legal de implementación de medidas de seguridad y la obligación de notificar al titular de los datos y a la autoridad de aplicación cuando acaece un incidente de seguridad.

Se regulan las transferencias internacionales y se establecen tres mecanismos con distinto nivel de jerarquía para realizar el flujo transfronterizo de datos personales con confianza.

Se establecen los derechos de los titulares de los datos comprendiendo, el derecho de acceso, el derecho de rectificación, el derecho de oposición y el derecho de supresión. Y se agregan los derechos a la portabilidad de datos personales y a la limitación y el derecho sobre las decisiones automatizadas y la elaboración de perfiles.

También, se establece la forma de ejercicio de los derechos, estableciendo que el ejercicio de cualquiera de ellos, no es requisito previo ni impide el ejercicio de otro.

El Responsable de tratamiento debe responder y, en su caso, satisfacer el pedido, dentro de los 10 días hábiles de haber sido intimado. Vencido el plazo sin que se satisfaga el pedido, o fuera insuficiente, queda expedito el trámite de protección de los datos personales ante la

Autoridad de Aplicación o, a elección de la persona Titular de los datos, la acción de Habeas Data.

Asimismo, se incorporan excepciones al ejercicio de los derechos, los cuales pueden ser limitados por ley en la medida en que ello sea necesario y proporcional para salvaguardar la seguridad pública, la defensa de la Nación, la protección de la salud pública, y las libertades de terceros y en resguardo del interés público.

Se prevé las obligaciones del Responsable y Encargado de tratamiento, entre ellas, las medidas para el cumplimiento de la responsabilidad proactiva; las políticas de tratamiento de datos personales; entre otras.

Se incorporan la figura del Delegado de Protección de Datos, la evaluación de impacto relativa a la protección de datos y los mecanismos de regulación vinculantes.

Se incorpora el Representante para los Responsables y Encargados que no estén establecidos en el país y la ley resulte de aplicación. Y se crea el Registro Nacional para la Protección de los Datos Personales.

Se establece como principio rector para la prestación de servicios de información crediticia que sólo pueden tratarse datos personales de carácter patrimonial relativos a la solvencia económica y al crédito.

Se indican las facultades de la Autoridad de Aplicación, los procedimientos y las sanciones a implementar en caso de constatar el incumplimiento de la ley. En relación a las multas, incorpora una unidad móvil sujeta a la variación del IPC y eleva los montos sustantivamente.

En lo relativo a la Autoridad de Aplicación, se propone un diseño institucional que supera el vigente.

Se crea una Agencia con autonomía funcional y autarquía financiera, a fin de no frustrar las intenciones y el espíritu de la ley. En este punto, debemos señalar que se vuelve al diseño ideado en el proyecto de ley sancionado por el Congreso de la Nación, posteriormente vetado por el Poder Ejecutivo Nacional, a través del Decreto 995/2000, que en los hechos, implicó eliminar todo tipo de independencia.

Se regula específicamente la acción judicial de habeas data. La mayor innovación consiste en la ampliación de la legitimación activa para acciones colectivas.

Se determina que las normas de la presente ley son de orden público y de aplicación en todo el territorio nacional, con excepción de las normas procesales, y se invita a las Provincias y a la Ciudad Autónoma de Buenos Aires a adherir.

La gravedad de la situación descripta marca la necesidad de urgente tratamiento por parte del Honorable Congreso de la Nación. El derecho a la protección de los datos personales es un derecho humano, y no puede estar sujeto su ejercicio a una normativa desactualizada.

Y esta urgencia también marca los desafíos que presenta la proyección de una normativa, la cual se presenta en diferentes planos. A nivel internacional, debe responder a los mejores estándares de protección de datos personales, y presentar coherencia y coordinación con la normativa a nivel regional. Además, a nivel local debe, por un lado, promover las ventajas de la tecnológica, y por el otro, velar por la protección de datos personales desde un enfoque de derechos humanos. Y si bien toda normativa es perfectible, el presente proyecto cumple con esos objetivos.

Por todo lo expuesto, solicito a mis pares el acompañamiento en la presente iniciativa legislativa.

Claudio M. Doñate