



PROYECTO DE LEY

*La Honorable Cámara de Diputados y el Senado de la Nación
Sancionan con Fuerza de Ley:*

LEY DE PROTECCIÓN DE 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, de conformidad con lo establecido en el artículo 43, párrafo Tercero de la CONSTITUCIÓN NACIONAL, los convenios internacionales que contengan disposiciones sobre protección de datos personales y los Tratados de Derechos Humanos en los que la REPÚBLICA ARGENTINA sea parte. Esta Ley establece las reglas para el debido tratamiento de los datos personales y la autodeterminación sobre la información personal, así como los derechos de las personas humanas 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, ya sea por el Responsable de tratamiento, Encargado de tratamiento o un Tercero, de una persona humana, sin esfuerzos o plazos desproporcionados o inviables, teniendo en cuenta factores como los costos y el tiempo necesario para la identificación o reidentificación de la persona a la luz de la tecnología disponible en el momento del tratamiento.

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 su información. Comprende un conjunto de principios y garantías relativas al legítimo tratamiento de sus datos personales.

Base de datos: Conjunto de datos cualquiera que fuera 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 puede denominar 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, o la persona titular de la responsabilidad parental, guarda o tutela en caso de niñas, niños y adolescentes, 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” la persona que puede ser identificada directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea, o por uno o varios elementos característicos de su identidad física, fisiológica, genética, biométrica, psíquica, económica, cultural o social de dicha persona.

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 identifican o hacen identificable de manera unívoca a una persona humana.

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, de cooperar con la Autoridad de Aplicación, y de 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: Sociedades controlantes, controladas y aquellas vinculadas en las cuales se tenga influencia significativa en las decisiones, denominación, domicilio, actividad principal, participación patrimonial, porcentaje de votos y, para las controlantes, principales accionistas. 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 pero compacto que responde a un mismo interés.

Incidente de seguridad de datos personales: Un suceso que, de forma real o inminente ponga en peligro la integridad, confidencialidad o disponibilidad de datos personales o de un sistema de información para el tratamiento de datos personales; o constituya una violación o amenaza inminente de violación de la ley, las políticas y los procedimientos de seguridad registrados por la Autoridad de Aplicación.

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

Seudonimización: El tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre 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 del tratamiento al que se refiere la presente Ley.

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

Tratamiento de datos: Cualquier operación o conjunto de operaciones, automatizada, parcialmente automatizada o no automatizada, realizada sobre datos personales, que permita, de manera enunciativa, la recolección, conservación, organización, estructuración, almacenamiento, modificación, relacionamiento, evaluación, bloqueo o destrucción, publicación 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, el ejercicio de la actividad periodística y las investigaciones por graves violaciones a los derechos humanos frente a crímenes de lesa humanidad, de conformidad con la normativa vigente en la materia.

En ningún caso se puede afectar el secreto de las fuentes de información periodística. Sin perjuicio del secreto de la fuente de información periodística, todo otro tratamiento de los datos personales por parte de organizaciones periodísticas o de organizaciones intermediarias de contenidos producidos por terceros que no sean estrictamente informativos, 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. Tampoco son aplicables las disposiciones establecidas en esta Ley a la información anónima ni 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 información 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 6°.- Principio de licitud, lealtad y transparencia. Los datos personales deben ser tratados de manera lícita, leal y transparente. El tratamiento se considera lícito si se realiza conforme a lo establecido en la presente Ley y normativa complementaria. Se considera leal si el Responsable de tratamiento se abstiene de tratar los datos a través de medios engañosos o fraudulentos. 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 no deben ser tratados de manera incompatible con estos.

No se considera incompatible con los objetivos iniciales el tratamiento ulterior de los datos personales 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.

El responsable no podrá negar el acceso a un producto o servicio, o establecer sobre ellos precios diferenciados, cuando el titular se oponga al tratamiento para finalidades distintas a las necesarias para la prestación del producto o servicio ofrecido.

ARTÍCULO 9º.- Principio de exactitud. Los datos personales objeto de tratamiento deben ser veraces, exactos, completos, comprobables y actualizados. Si fuera necesario actualizarlos, se deben adoptar todas las medidas razonables para que no se altere su veracidad.

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

En los casos en que los datos son proporcionados por su titular se presume su exactitud.

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.- 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, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone la presente Ley con el fin de proteger los derechos de la persona Titular de los datos.

ARTÍCULO 12.- Principio de responsabilidad proactiva y demostrada. El Responsable y el Encargado de tratamiento de los datos personales 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 mismos, el cumplimiento de las obligaciones dispuestas por la presente Ley y que permitan 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 solo 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, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos de la persona Titular de los datos, y esta se encontrara imposibilitada de otorgar el consentimiento por sí o por sus representantes;
- f) Que sea necesario para la satisfacción del interés legítimo del Responsable de tratamiento, siempre que previamente comunique al titular del dato su intención de realizar un procesamiento informado y justificado en esta base legal para que pueda ejercer sus derechos, y 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 del cumplimiento de las disposiciones de la presente Ley, la Autoridad de Aplicación podrá requerir al Responsable de tratamiento el análisis previo que fundamenta el tratamiento de los datos personales para la satisfacción de un interés legítimo, y el Responsable de tratamiento deberá ser capaz de demostrar la existencia del interés legítimo, la necesidad de recolectar o tratar los datos en cada caso, y los criterios de razonabilidad y proporcionalidad considerados para acotar dicho tratamiento, teniendo para sí la carga de la prueba.

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.

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

Cuando los datos personales hayan sido obtenidos sin el correcto consentimiento del titular y/o de manera engañosa o fraudulenta, el Responsable del tratamiento será pasible del régimen de sanciones establecido en el Capítulo VIII de esta ley.



ARTÍCULO 15.- Revocación del consentimiento. La persona Titular de los datos puede revocar el consentimiento en cualquier momento y sin necesidad de fundamentar la petición. Dicha revocación no tiene efectos retroactivos.

El Responsable de tratamiento debe proveer para la revocación mecanismos sencillos, gratuitos, expeditos y, al menos, 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, al menos, la siguiente información:

- a) Nombre o razón social, domicilio y medios electrónicos de contacto del Responsable 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 la REPÚBLICA ARGENTINA, 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 y el procedimiento a través del cual puede ejercerlo;
- 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 en caso de que el Responsable o el Encargado de tratamiento incumpla con la presente Ley.

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 la persona Titular de los datos o si la base legal que ha utilizado para legitimar el tratamiento no ha sido el consentimiento de la persona Titular de los datos.

Si los datos no han sido obtenidos de la persona Titular de los datos, 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 las ocasiones en que los datos se utilicen para comunicarse con la persona Titular de los datos se debe proveer la información al momento de la primera comunicación, y si son cedidos a otro destinatario se debe informar a la persona Titular de los datos en la primera cesión.

ARTÍCULO 17.- Tratamiento de datos sensibles. En el tratamiento de datos sensibles se debe implementar la responsabilidad reforzada que implica, entre otras características, mayores niveles de seguridad, confidencialidad, restricciones de acceso, uso y circulación.

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;
- 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 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 pseudoanonimización;

g) Tuviera una finalidad estadística, o fuera realizada por el propio responsable de recabar esos datos, 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. De manera general, sólo se podrá exceptuar el consentimiento a efectos de responder a sucesos repentinos de salud pública o para proteger la vida y la salud de las personas humanas o la seguridad de sus bienes. El Responsable deberá justificar adecuadamente las condiciones de emergencia, y una vez cesada la emergencia se eliminarán los datos, o bien se obtendrá el debido consentimiento y/o se practicarán las notificaciones requeridas.

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

ARTÍCULO 18.- Tratamiento de datos del sector público.

El tratamiento de datos personales realizado por el sector público debe fundarse en alguna de las bases legales establecidas en el artículo 13 y cumplir con todos los principios y condiciones que definen la licitud para el tratamiento determinadas en la presente Ley, entre ellos con los estándares internacionales de derechos humanos aplicables a la materia y los principios de legalidad, proporcionalidad y necesidad.

Las cesiones de datos personales efectuadas por organismos del Sector Público deben implementarse mediante un acuerdo entre cedente y cesionario. El mismo 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.

La entidad cedente deberá haber obtenido los datos de acuerdo a una base legal establecida en el Artículo 13 de esta ley y en el ejercicio de sus competencias asignadas por ley.

Los datos involucrados en las cesiones o transferencias serán únicamente los adecuados y estrictamente necesarios para acometer la finalidad pública de acuerdo a las competencias legales vigentes del cesionario, de conformidad con el principio de minimización. Se prohíbe la cesión masiva e indiscriminada de bases de datos. Cumplida la finalidad que motivó el acuerdo de cesión de datos, el cesionario deberá suprimir los datos o la autoridad cedente revocar el acceso a la base compartida. No serán aplicables estas reglas a las transferencias de datos sensibles realizadas entre entidades que cumplen las mismas funciones en distintas esferas del estado.

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.

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

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

a) En los casos de ejecución descentralizada de actividades públicas que requieran la transferencia, exclusivamente para este fin específico y particular, siguiendo lo dispuesto en la Ley de Acceso a la Información Pública;

b) Cuando así lo establezca una ley, y la transferencia esté respaldada por contratos, convenios o instrumentos análogos debidamente publicados.

La autoridad de aplicación podrá, en cualquier momento, solicitar a las entidades públicas información específica sobre el alcance y naturaleza de los datos, detalles sobre el tratamiento realizado, la adopción de medidas dirigidas a garantizar la seguridad de los datos y emitir opiniones técnicas complementarias para garantizar el cumplimiento de la ley. También podrá establecer reglas complementarias para el



cumplimiento de los deberes de información y para el uso compartido de datos personales.

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.

La Autoridad de Aplicación dispondrá la adopción de mecanismos simplificados para el ejercicio de los derechos consagrados en la presente ley, y bregará por la designación de un Delegado de Protección de Datos Personales en cada autoridad u organismo público según lo dispuesto en el Artículo 44 de la presente ley.

ARTÍCULO 19.- Tratamiento de datos de niñas, niños y adolescentes. En el tratamiento de datos personales de niñas, niños y adolescentes, se debe privilegiar la protección del interés superior de estos y el ejercicio progresivo de sus derechos, conforme a la Convención sobre los Derechos del Niño, aprobada por la Ley N° 23.849, a los demás instrumentos internacionales de los que la Nación es parte que tiendan a garantizar su bienestar y protección integral, al Código Civil y Comercial de la Nación, y a la Ley N° 26.061 y normas complementarias.

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 otorgó el consentimiento. En tales casos, el Responsable de tratamiento deberá arbitrar procesos que permitan verificar, de manera razonable, que el consentimiento haya sido otorgado por la persona titular de la responsabilidad parental o por quien se encuentre a cargo de su ejercicio o de la guarda o tutela sobre la niña, el niño o adolescente menor de DIECISÉIS (16) años.

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.

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 y mentales del usuario, con el uso de recursos audiovisuales cuando corresponda.

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 por sí o por sus representantes.

Es tarea del Estado y de las entidades educativas 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.- Principio de seguridad de los datos personales. El Responsable y el Encargado de tratamiento de datos personales deben sujetarse al principio de seguridad 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 y confidencialidad 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, y las mejores prácticas de seguridad integral de acuerdo a la naturaleza, el alcance, el contexto y los fines del tratamiento.

El Responsable y el Encargado de tratamiento deben adoptar las medidas de seguridad aplicables a los datos personales que trate, y considerar, al menos, los siguientes factores:

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.

El Responsable y el Encargado de tratamiento de datos personales deben evidenciar que las medidas adoptadas e implementadas evitan la materialización de los riesgos identificados.

ARTÍCULO 21.- Notificación de incidentes de seguridad. 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 ante la Autoridad de Aplicación la extensión del plazo, justificando de manera objetiva y fundada dicha necesidad.

De igual manera, el Responsable de tratamiento debe 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, en la medida en que la misma sea igualmente efectiva para informar a la persona Titular de los datos de la incidencia.

La notificación debe contener, al menos, 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;

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.

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 definitiva. En caso de que no sea posible enviar toda la información detallada al mismo



tiempo, la persona responsable deberá enviarla a medida que sea posible y sin dilación alguna que le sea imputable.

ARTÍCULO 22.- Deber de confidencialidad. El Responsable de tratamiento, el Encargado y las demás personas que intervengan en cualquier fase del tratamiento están obligados a la confidencialidad respecto de los datos personales. Esta obligación subsiste aun después de finalizada su relación con la persona Titular de los datos, el Responsable o el Encargado de tratamiento, según corresponda. 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, según lo estipulado por el Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal y sus posteriores modificaciones, y lo determinado por el artículo 24 de la presente ley;
- b) Si el 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.

A efectos de demostrar que la transferencia internacional sea realizada conforme a lo que establece esta Ley, la carga de la prueba recae, en todos los casos, en el exportador.

Como principio general regirá el criterio de reciprocidad frente a medidas adoptadas por otros Estados en el marco de transferencias de datos.

Quien realiza transferencias internacionales de datos 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 de la presente Ley, la condición de país 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 el respeto de los derechos de protección de datos personales;
- d) La existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el país u organización que reciba 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, y a falta de una decisión de adecuación, 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 en los términos que establece la presente Ley;

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

En los casos de transferencias regidas por el presente artículo, el acuerdo o mecanismo que instrumente la transferencia, debe reconocer que la parte exportadora se encuentra sujeta a la jurisdicción de la Autoridad de Aplicación y de los tribunales de la REPÚBLICA ARGENTINA competentes y asegurar que la parte importadora 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 efectivas para proteger sus derechos.

ARTÍCULO 26 - Excepciones. 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, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos de la persona Titular de los datos y esta se encontrara imposibilitada de otorgar su consentimiento por sí o por sus representantes.

Las condiciones establecidas en el presente artículo deben estar siempre sujetas al cumplimiento de los estándares internacionales de derechos humanos aplicables a la materia, al cumplimiento de los principios de esta Ley y a los criterios de legalidad, proporcionalidad y necesidad.

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.

Cuando la transferencia sea necesaria por razones de interés público deberá ser publicada y cumplir los requisitos en los mismos términos dispuestos por el Artículo 18 de esta ley.

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 y, en tal caso, a solicitar información y obtener confirmación de ello. 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 traten;
- c) Los destinatarios o las categorías de destinatarios a los que se cedieron o se prevean ceder los datos personales;
- d) La relativa 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) La existencia del derecho a solicitar del Responsable de Tratamiento 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 o semiautomatizadas, incluida la elaboración de perfiles a que se refiere el artículo 31 de la presente Ley y, al menos en tales casos, información significativa sobre la lógica aplicada.



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. La información debe ser suministrada en forma clara, completa, exenta de codificaciones y, en su caso, acompañada de una explicación de los términos que se utilicen, en lenguaje de fácil comprensión y de preferencia accesible en la lengua de su elección.

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 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 al tratamiento de sus datos personales si tuvieran por objeto la publicidad, la prospección comercial o la mercadotecnia directa, incluida la elaboración de perfiles. Cuando la persona Titular de los datos se oponga al tratamiento para esos propósitos, sus datos personales deben dejar de ser tratados.

La persona Titular de los datos tiene derecho a que el tratamiento de datos personales se limite a su almacenamiento durante el período que medie entre una solicitud de rectificación u 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.

La supresión tampoco procede si el dato es necesario para el esclarecimiento de casos de graves 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 basada única o parcialmente en el tratamiento automatizado o semiautomatizado de datos, incluida la elaboración de perfiles e inferencias, que le produzca efectos jurídicos. Se entiende por decisiones parcialmente automatizadas o semiautomatizadas a aquellas en las que no hay intervención humana significativa.

El interesado tiene derecho a solicitar información sobre los criterios de valoración del programa automatizado o semiautomatizado aplicado, a la revisión por una persona humana de las decisiones tomadas sobre la base del tratamiento automatizado o semiautomatizado que afecten sus intereses, incluidas las decisiones encaminadas a definir sus aspectos personales, profesionales, de consumo, de crédito, de su personalidad u otros, y a la impugnación de la decisión ante el responsable o encargado del tratamiento.



El Responsable de tratamiento debe proporcionar a la persona titular de los datos, 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, así como cumplimentar con lo dispuesto en el párrafo anterior cuando corresponda.

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, particularmente si se encuentran basados en alguna de las categorías de datos contenidas en la definición de datos sensibles del artículo 2 de la presente Ley.

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 información personal.

ARTICULO 32.- Datos inferidos. Se entenderá por dato inferido aquella información relativa a un individuo identificado o identificable, creada a través de razonamiento o deducción y no sólo mediante la mera observación o recolección de sus datos personales. Los datos inferidos son datos personales en los términos de esta ley y, por lo tanto, quedan comprendidos en sus previsiones y sujetos a todos los derechos y garantías que ésta otorga, independientemente de que supongan o no un daño o perjuicio al titular. Esto incluye, pero no se limita a, los derechos de acceso, rectificación, cancelación y oposición.

Será lícita su producción y tratamiento siempre que el Responsable pueda explicar justa y suficientemente el proceso lógico utilizado a tal efecto, de acuerdo con el artículo 27 i) de esta ley.

ARTÍCULO 33.- 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.

Sin perjuicio de otros derechos de la persona Titular de los datos, el derecho a la portabilidad de los datos personales 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 con base en los datos personales de la persona titular.

ARTÍCULO 34.- Derecho de limitación. La persona interesada 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 la persona Titular de los datos 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 la persona interesada 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 la persona interesada los necesita para la formulación, el ejercicio o la defensa de sus derechos;
- d) Si la persona interesada se ha opuesto al tratamiento en virtud del artículo 29 de la presente Ley, mientras se verifica si los motivos legítimos del Responsable de tratamiento prevalecen sobre los de la persona interesada.

Toda persona interesada que haya obtenido la limitación del tratamiento debe ser informada por el Responsable de tratamiento antes del levantamiento de dicha limitación.

En el caso en que la persona Titular de los datos recurra ante la Autoridad de Aplicación por la negativa del Responsable o Encargado de tratamiento, esta limitación se extenderá hasta la resolución del procedimiento administrativo.

ARTÍCULO 35.- 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. El derecho a la protección de los datos personales y los derechos derivados del mismo



son personalísimos e irrenunciables. Será nula de pleno derecho toda estipulación en contrario. El Responsable de tratamiento debe responder y, en su caso, satisfacer los derechos de la persona Titular de los datos dentro de los DIEZ (10) días hábiles de haber recibido la solicitud.

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 de esta Ley o, a elección de la persona Titular de los datos, puede interponer la acción de Habeas Data prevista en el artículo 66 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.

El ejercicio de los derechos previstos en esta Ley en el caso de las personas Titulares de los datos fallecidas les 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.

El derecho de acceso a que se refiere el artículo 27 de la presente Ley solo puede ser ejercido en forma gratuita a intervalos superiores a SEIS (6) meses. Si se ejerce en intervalos inferiores a dicho plazo, 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, salvo que la solicitud sea fundada en justa causa. 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 enumerados en este Capítulo 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. El Responsable de tratamiento tiene la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

ARTÍCULO 36.- Excepciones al ejercicio de los derechos. Los derechos y las garantías establecidos en esta Ley 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 deben ser reconocidas de manera expresa mediante una norma de rango legal, salvaguardando la integridad de los datos personales y



restringiendo su uso estricto a los fines que persiga dicha norma, con el propósito de brindar certeza suficiente a las personas Titulares de los datos acerca de la naturaleza y los alcances de la medida.

Cualquier norma de rango constitucional o legal que tenga como propósito limitar los derechos consagrados en el Capítulo IV de esta ley deberá 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.

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.

Las limitaciones previstas en este artículo deben ser las necesarias, adecuadas y proporcionales en una sociedad democrática, y deben respetar los derechos y las libertades fundamentales de las personas Titulares de los datos.

CAPÍTULO V - OBLIGACIONES DE LOS RESPONSABLES Y ENCARGADOS DE TRATAMIENTO

ARTÍCULO 37.- Deberes del Responsable de tratamiento. Los Responsables de tratamiento deben cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente Ley, las normas reglamentarias y otras que rijan su actividad:

- 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, especialmente los derechos de las personas Titulares de los datos y la materialización de los principios del tratamiento de datos personales;

b) Garantizar a la persona Titular de los datos, en todo tiempo, el pleno y efectivo ejercicio del derecho de protección de datos, especialmente conocer, actualizar, rectificar, suprimir sus datos personales u oponerse al tratamiento de estos;

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 a la Autoridad de Aplicación y a las personas Titulares de los datos 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 entre el Responsable y 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 conforme a los requisitos de la presente Ley 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 la información de la persona Titular de los datos;

m) En caso de que corresponda, designar un Delegado de Protección de Datos. En caso de no corresponder, se debe establecer una persona o área que asuma la función de protección de datos personales y de 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 responden por la observancia de aquellas ante la Autoridad de Aplicación y la persona Titular de los datos de que se trate. 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.

ARTÍCULO 38.- Deberes del Encargado de tratamiento. Los Encargados de tratamiento deben cumplir con los siguientes deberes al realizar el tratamiento de datos personales, sin perjuicio de las demás disposiciones previstas en la presente Ley, las normas reglamentarias y otras que rijan su actividad:

- a) La prestación de servicios de tratamiento de datos por cuenta de terceros entre un Responsable y un Encargado de tratamiento debe quedar formalizada mediante un contrato por escrito y no requiere del consentimiento de la persona Titular de los datos;
- b) El Encargado de tratamiento debe limitarse a llevar a cabo solo aquellos tratamientos de datos encomendados por el Responsable de tratamiento;
- c) Los datos personales objeto de tratamiento deben aplicarse o utilizarse con el fin que figure en el contrato, y no deben ser cedidos a otras personas, ni aún para su conservación, salvo autorización expresa del Responsable de tratamiento;
- d) Una vez cumplida la prestación contractual, los datos personales tratados deben ser devueltos al Responsable de tratamiento o destruidos, salvo que medie autorización expresa del Responsable de tratamiento cuando razonablemente se pueda presumir la posibilidad de ulteriores encargos, en cuyo caso solo podrán conservarse por un máximo de DOS (2) años;
- e) Debe permitirse 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) Deben implementarse medidas apropiadas, útiles, oportunas, pertinentes y eficaces para garantizar y poder demostrar el adecuado cumplimiento de la presente Ley y sus normas reglamentarias, especialmente los derechos de las personas Titulares de los datos y la materialización de los principios del tratamiento de datos personales;



- g) Deben tratarse los datos personales bajo condiciones de seguridad apropiadas para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;
- h) Deben cumplirse las instrucciones, órdenes o requerimientos que imparta la Autoridad de Aplicación;
- i) Deben tramitarse 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) Debe informarse en el plazo de Ley a la Autoridad de Aplicación y al Responsable de tratamiento cuando se presenten incidentes de seguridad y existan riesgos en la administración de la información de las personas Titulares de los datos;
- k) En caso de que corresponda, debe designarse un Delegado de Protección de Datos. En caso de no corresponder la designación de un Delegado de Protección de Datos, debe establecerse una persona o área que asuma la función de protección de datos personales y trámite de 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. Para el supuesto en que el subcontratado incumpla sus obligaciones y responsabilidades respecto al tratamiento de datos que lleve a cabo conforme a lo estipulado en el contrato, asume la calidad de Responsable de tratamiento en los términos y condiciones previstos en la presente Ley.

Los contratos previstos en este artículo 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 del Responsable y del Encargado de tratamiento.

ARTÍCULO 39.- 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 deben instrumentarse utilizando los medios idóneos disponibles para informar a la persona Titular de los datos, en un lenguaje claro y sencillo, y deben incluir la información detallada en el artículo 16 de la presente Ley y la fecha de su entrada en vigencia.

En caso de que la base legal para el tratamiento sea el consentimiento de la persona Titular de los datos y se realicen cambios sustanciales en el contenido de estas



políticas, los Responsables y Encargados de tratamiento deben notificar y obtener una nueva autorización para el tratamiento de los datos.

ARTÍCULO 40.- Medidas para el cumplimiento de la responsabilidad proactiva. Las medidas adoptadas para el cumplimiento de las disposiciones de la presente Ley 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 para atender el 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 conforme a lo establecido en la presente Ley.

Las medidas de responsabilidad proactiva deben quedar documentadas y a disposición de la Autoridad de Aplicación en caso de ser requeridas. La implementación efectiva de estas medidas debe ser tomada en cuenta como un factor de atenuación para la graduación de la sanción por una eventual violación de la presente Ley y/o de sus normas reglamentarias.

ARTÍCULO 41. - Protección de datos desde el diseño y por defecto. El Responsable de tratamiento y el Encargado deben, desde la etapa del diseño de productos y servicios, y antes del tratamiento, prever y aplicar medidas tecnológicas y organizativas apropiadas para cumplir los principios y garantizar los derechos de las personas Titulares de los datos establecidos en esta Ley. Estas medidas deben ser adoptadas teniendo en cuenta el estado de la tecnología y la naturaleza, ámbito, contexto y fines del tratamiento de los datos, así como los riesgos que entraña el tratamiento para el derecho a la protección de los datos de sus titulares.

El Responsable de tratamiento debe aplicar las medidas tecnológicas y organizativas apropiadas 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. Tales medidas deben garantizar que, por defecto, los datos personales

no sean accesibles, sin la intervención de la persona Titular de los datos, a un número indeterminado de personas humanas.

ARTÍCULO 42.- 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 amparados en la presente Ley, deberá realizar, de manera previa a la implementación del tratamiento, una evaluación del impacto relativa a la protección de los datos personales.

Esta evaluación es obligatoria en los siguientes casos, sin perjuicio de otros que establezca la Autoridad de Aplicación:

- 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.

ARTÍCULO 43.- 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 a que se refiere el inciso a) del artículo 41 de la presente Ley;
- d) Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de los datos personales, y para demostrar la conformidad con la presente Ley, teniendo en cuenta los derechos e intereses legítimos de los Titulares de los datos y de otras personas que pudieran verse potencialmente afectadas.

ARTÍCULO 44.- Informe previo. Cuando una 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) 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 sobre el informe.

ARTÍCULO 45.- Delegado de Protección de Datos. Los Responsables y Encargados de tratamiento deben designar un Delegado de Protección de Datos en cualquiera de 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, conforme a lo que se establezca en esta Ley, en la reglamentación o en la normativa que dicte al respecto la Autoridad de Aplicación.

Si los Responsables y Encargados de tratamiento no se encuentran obligados a la designación de un Delegado de Protección de Datos, de acuerdo a lo previsto en este artículo, pueden designar uno de manera voluntaria.

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 tamaño y 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.

El rol de Delegado de Protección de Datos puede ser desempeñado por un empleado del Responsable o Encargado de tratamiento o en el marco de un contrato de prestación de servicios. El Delegado de Protección de Datos puede ejercer otras funciones siempre que no den lugar a conflictos de intereses.

El Responsable o Encargado de tratamiento está obligado a respaldar al Delegado de Protección de Datos en el desempeño de sus funciones, y a facilitarle los recursos necesarios para su desempeño y para el mantenimiento de sus conocimientos especializados y la actualización de estos.

El Delegado de Protección de Datos debe ejercer sus funciones de manera autónoma y libre de interferencias, sin recibir instrucciones, y solo debe responder ante el más alto nivel jerárquico de la organización. No puede ser destituido ni sancionado por el correcto desempeño de sus funciones.

La autoridad de aplicación podrá establecer reglas complementarias sobre la definición, los requisitos y las funciones del delegado de protección de datos,

ARTÍCULO 46.- Funciones del Delegado de Protección de Datos. El Delegado de Protección de Datos tiene las siguientes funciones, sin perjuicio de otras que se le asignen especialmente:

- 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 47.- Representantes de Responsables y Encargados de tratamiento. Cuando el Responsable o el Encargado de tratamiento no se encuentren establecidos en la REPÚBLICA ARGENTINA, conforme a lo normado en el artículo 4°, inciso b de la presente Ley, deberán designar un Representante en el territorio nacional, quien actuará en nombre de ellos.

El presente artículo no será aplicable cuando:

- a) El tratamiento sea ocasional;
- b) Se trate de organismos públicos extranjeros.

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. También puede ser objeto de un procedimiento sancionatorio ante el incumplimiento por parte del Responsable o del Encargado de tratamiento. En caso de falta de respuesta por parte del Responsable o Encargado de tratamiento, el Representante será responsable por cualquier sanción impuesta en el marco de dicho procedimiento.

ARTÍCULO 48.- 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, conforme al artículo 44 de la presente Ley, deban tener un Delegado de Protección de Datos.
- b) Los Responsables y Encargados de tratamiento de datos que, conforme lo establecido en el artículo 46 de la presente Ley, 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 49 - Promoción y reconocimiento de buenas prácticas. La Autoridad de Aplicación promoverá y ponderará de manera positiva las buenas prácticas de empresas y organizaciones 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, sellos de confianza, certificaciones u otros mecanismos que coadyuven a contribuir con el objetivo señalado.

Las asociaciones u otras entidades representativas de categorías de Responsables o Encargados de tratamiento pueden adoptar estos mecanismos de gestión con carácter vinculante para todos sus miembros. Podrán ser puestos en conocimiento de la Autoridad de Aplicación, la cual determinará si se adecúan a las disposiciones de esta Ley y, en su caso, los reconocerá o sugerirá las correcciones que estime necesarias a efectos de su reconocimiento como “buena práctica adecuada a la Ley Nacional de Protección de Datos Personales”. Los que resulten reconocidos serán registrados y dados a publicidad por la Autoridad de Aplicación.

CAPÍTULO VI - PROTECCIÓN DE DATOS DE INFORMACIÓN CREDITICIA

ARTÍCULO 50.- Protección de datos de información crediticia del sector financiero y no financiero. En la prestación de servicios de información crediticia solo 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 parientes 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 51.- Plazo de conservación de la información crediticia. Solo 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 un (1) año 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 52.- 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 comunicar a la persona Titular de los datos 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.



Las entidades crediticias, financieras, y cualquier otro acreedor, 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, así como la empresa que proveyó dicho informe, y hacerle entrega de una copia.

ARTÍCULO 53.- 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. Toda modificación debe ser comunicada por las entidades crediticias 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 54.- Autoridad de Aplicación. La Autoridad de Aplicación de la presente Ley es la AGENCIA DE PROTECCIÓN DE LOS DATOS PERSONALES, como ente autárquico que funcionará con autonomía funcional en el ámbito de la JEFATURA DE GABINETE DE MINISTROS.

La conducción de la Agencia estará a cargo de un o una Director o Directora a designar por el Poder Ejecutivo nacional mediante un procedimiento de selección público, abierto y transparente que garantice la idoneidad del candidato.

El procedimiento de selección del Director o Directora, su rango y jerarquía, y los requisitos e incompatibilidades para la postulación y el ejercicio del cargo son similares a los dispuestos por los artículos 21, 22 y 23 de la Ley 27.275.

ARTÍCULO 55.- Facultades de la Autoridad de Aplicación.

La Autoridad de Aplicación tendrá las siguientes funciones y atribuciones:



- a) Ejercer la supervisión, control y evaluación de las actividades efectuadas por el Responsable y Encargado de tratamiento de datos personales. En el caso de que para tal fin se requiera el auxilio de la fuerza pública, puede solicitar autorización judicial para acceder a locales, equipos o programas de tratamiento de datos;
- b) Dictar las normas complementarias y criterios orientadores que se deben observar en el desarrollo de las actividades comprendidas por esta Ley;
- c) Tramitar los requerimientos y denuncias interpuestos en relación con el tratamiento de datos en los términos de la presente Ley, 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 los antecedentes, documentos, programas u otros elementos relativos al tratamiento de datos que se les requieran. En estos casos, la Autoridad de Aplicación debe 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 los derechos de las personas Titulares de los datos, 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 se promovieren por violaciones a la presente Ley;
- 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;
- ll) 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;
- m) Asistir, asesorar y capacitar a las personas y entidades, públicas y privadas, acerca de los alcances de la presente Ley;
- n) Promover la cultura de la privacidad, el debido tratamiento de datos y la autodeterminación informativa, así como una gestión responsable, ética y transparente del procesamiento automatizado;
- ñ) Desarrollar investigación aplicada y conocimiento sobre la protección de datos personales;
- o) Promover, organizar y desarrollar programas tendientes a la protección de datos personales de niños, niñas y adolescentes en internet, juegos electrónicos y otras plataformas digitales;
- p) Divulgar los derechos de las personas Titulares de los datos en relación con el tratamiento de datos personales, e implementar campañas pedagógicas para capacitar e informar a los ciudadanos, Responsables y Encargados de tratamiento acerca del ejercicio y garantía del derecho fundamental a la protección de datos;
- q) Generar estrategias para la prevención de la violencia digital en relación con la defensa de la privacidad y tratamiento de datos;
- r) Promover la incorporación de contenidos educativos vinculados al tratamiento de datos, la privacidad y la autodeterminación informativa;
- s) Promover la capacitación y formación profesional en materia de protección de datos personales;
- t) Convocar a un Consejo Asesor con integración de representantes provinciales, de fuerzas políticas con representación de los cuatro mayores bloques de la Cámara de Diputados de la Nación y de agremiaciones empresariales, profesionales y sindicales, de acuerdo a la reglamentación;
- u) Ejercer otras facultades que le sean asignadas por la Ley o su Reglamentación.

CAPÍTULO VIII - PROCEDIMIENTOS Y SANCIONES

ARTÍCULO 56.- 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 un tercero, asociaciones u organizaciones, siempre que exista un interés legítimo, por denuncia de violaciones a la presente Ley;
- c) De oficio.

En los procedimientos contemplados en los incisos b) y c) se aplicará la Ley Nacional de Procedimientos Administrativos N° 19.549 y sus modificatorias. Para el caso del procedimiento previsto en el inciso a) del artículo citado, la mencionada Ley N° 19.549 será de aplicación supletoria.

ARTÍCULO 57.- Trámite de protección de los datos personales. Para el procedimiento indicado en el inciso a) del artículo 56 de la presente Ley, 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, y acreditando haber efectuado la intimación prevista en el artículo 34 de esta Ley.

La presentación debe realizarse dentro de los TREINTA (30) días hábiles siguientes a la fecha en que se comunique la respuesta a la persona Titular de los datos por parte del Responsable o Encargado de tratamiento, de acuerdo a lo previsto en el artículo 35, o en cualquier momento si el plazo allí establecido hubiere vencido sin respuesta del Responsable o Encargado de tratamiento.

La Autoridad de Aplicación intimará a los Responsables o Encargados de tratamiento para que en el plazo de QUINCE (15) días hábiles emitan respuesta, ofrezcan las pruebas que estimen pertinentes y manifiesten por escrito lo que a su derecho convenga. En caso de ser solicitado, de manera fundada y con anterioridad al vencimiento del plazo inicial, la Autoridad de Aplicación podrá otorgar una prórroga por el mismo término que el plazo inicial.

Concluida la recepción de las pruebas, se procederá a labrar un Acta en la que se dejará constancia del hecho denunciado y/o verificado, las infracciones constatadas



y las normas presuntamente infringidas. Dicha Acta se debe notificar al Responsable o Encargado de tratamiento haciéndole saber que le asiste el derecho a presentar su descargo dentro de los CINCO (5) días hábiles de notificado.

ARTÍCULO 58.- 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 la presente Ley. La Autoridad de Aplicación dictará la resolución que corresponda dentro de un plazo razonable establecido en la reglamentación y normativa complementaria, atendiendo a la complejidad del tema a resolver.

ARTÍCULO 59.- 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 60.- Recursos. Contra las resoluciones emitidas por la Autoridad de Aplicación en los procedimientos contemplados en el artículo 56 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. No procede el recurso de alzada.

Las resoluciones de la Autoridad de Aplicación agotan la vía administrativa a los efectos de lo previsto en la Ley Nacional de Procedimientos Administrativos N° 19.549 y sus modificatorias, y pueden ser impugnadas ante el fuero en lo Contencioso Administrativo Federal.

ARTÍCULO 61.- 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.

Las obligaciones con efecto correctivo a implementar podrán consistir en medidas técnicas, jurídicas, organizativas, educativas o administrativas que la Autoridad de



Aplicación considere pertinentes, según las circunstancias particulares del caso, para garantizar un tratamiento adecuado de datos personales.

ARTÍCULO 62.- 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 al presente artículo.

ARTÍCULO 63.- Determinación de la unidad móvil. La Autoridad de Aplicación podrá establecer multas sobre la base de la unidad de cuenta definida en la presente Ley. El valor inicial de la unidad móvil se establece en PESOS CIEN MIL (\$ 100.000), y debe ser actualizado semestralmente 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 64.- 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 CUATRO POR CIENTO (4 %) de la facturación total anual global del infractor en el ejercicio financiero anterior a la aplicación de la sanción.

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.



La Autoridad de Aplicación se encuentra facultada para dictar las normas complementarias y/o aclaratorias a tales fines. También determinará las infracciones que serán consideradas leves, graves y gravísimas, y los topes de las multas aplicables en cada caso.

ARTÍCULO 65.- 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 público, puede imponer medidas correctivas con el fin de subsanar y mitigar los efectos producidos por el incumplimiento de la presente Ley. Entre ellas, la obligación de documentar los procedimientos establecidos para el tratamiento de los datos personales; de formular planes de responsabilidad y cumplimiento, capacitación especializada y formación profesional obligatoria en la materia para el personal de los organismos; o de implementar mejoras de infraestructura y medidas de seguridad, entre otras.

Las infracciones a la presente Ley por parte de los organismos públicos serán pasibles de las sanciones previstas en el artículo 61 de esta Ley, excepto la del inciso b), sin perjuicio de la aplicación de las sanciones civiles, disciplinarias y penales de los artículos 117 bis y 157 bis del CÓDIGO PENAL DE LA NACIÓN ARGENTINA respecto de las funcionarias públicas y los funcionarios públicos responsables.

ARTÍCULO 66.- Graduación. Las sanciones a las que se refiere el artículo 62 de la presente Ley deben ser graduadas, respetando el debido proceso legal y según las peculiaridades del caso específico, 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;
- ll) Otros que pueda considerar la Autoridad de Aplicación, según la naturaleza del caso.

CAPÍTULO IX - ACCIÓN DE HABEAS DATA

ARTÍCULO 67.- 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 presente Ley o la Constitución Nacional por parte de Responsables o Encargados de tratamiento.

ARTÍCULO 68.- Legitimación activa y pasiva. La acción de habeas data podrá ser ejercida por el Titular de los datos afectados, sus tutores, representantes legales o curadores. 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 será notificada del inicio de la acción.

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. En tal caso, los promotores de estas acciones 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. Excepcionalmente, estos podrán interponer la acción contra otros Responsables o Encargados de tratamiento cuando los últimos incumplan con sus obligaciones legales o convencionales y esto pueda acarrearles perjuicio.



ARTÍCULO 69.- Competencia. Es competente para entender en la acción de habeas data el juez del domicilio del actor o del demandado, a elección del actor. 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 70.- Procedimiento aplicable. La acción de habeas data tramita según las disposiciones de la presente Ley y, supletoriamente, según el procedimiento que corresponde a la acción de amparo común y según las normas procesales en lo atinente al juicio sumarísimo. El Juez dispone de amplias facultades para adaptar los procedimientos de acuerdo a las circunstancias particulares del caso y con el fin de dar mayor eficacia tuitiva al proceso.

ARTÍCULO 71.- Requisitos de la demanda. La demanda 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. En el caso de bases de datos públicas, 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 entienda que se esté efectuando tratamiento de datos referido a su persona y los motivos por los cuales considere que procede el ejercicio de los derechos que le reconoce la presente Ley. Asimismo, deberá justificar el cumplimiento de los recaudos que hacen al ejercicio de tales derechos.

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 la base de datos en lo referente a los datos personales motivo del juicio cuando sea manifiesto el carácter ilícito del tratamiento de esos datos o ellos sean inequívocamente falsos o inexactos.

ARTÍCULO 72.- Trámite. Admitida la acción, el Juez debe requerir al Responsable o Encargado de tratamiento la remisión de la información concerniente al accionante y el ofrecimiento de la prueba pertinente. 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, pero podrá ser ampliado prudencialmente por el Juez.

Los Responsables o Encargados de tratamiento no pueden alegar la confidencialidad de la información que se les requiere, 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 73.- Contestación del informe. Al contestar el informe, el Responsable o Encargado de tratamiento de datos 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 74.- Ampliación de la demanda. Contestado el informe, la parte actora puede, en el término de TRES (3) días, ampliar el objeto de la demanda y ofrecer, en el mismo acto, la prueba pertinente. De esta presentación se debe dar traslado a la parte demandada por igual término para que conteste y ofrezca prueba.

ARTÍCULO 75.- 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. La sentencia deberá ser comunicada a la Autoridad de Aplicación.

De estimarse procedente la acción, se especificará si la información debe ser bloqueada, suprimida, rectificada o actualizada, estableciendo un plazo para su cumplimiento.

El rechazo de la acción no constituye presunción respecto de la responsabilidad en que hubiera podido incurrir la parte demandada.

Contra la sentencia procede el recurso de apelación.

CAPÍTULO X – SANCIONES ADMINISTRATIVAS



ARTÍCULO 76. - Sanciones administrativas.

1. Sin perjuicio de las responsabilidades administrativas que correspondan en los casos de responsables o usuarios de bancos de datos públicos; de la responsabilidad por daños y perjuicios derivados de la inobservancia de la presente Ley, y de las sanciones penales que correspondan, el organismo de control podrá aplicar las sanciones de apercibimiento, suspensión, multa, clausura o cancelación del archivo, registro o banco de datos.
2. La reglamentación determinará las condiciones y procedimientos para la aplicación de las sanciones previstas, las que deberán graduarse en relación con la gravedad y extensión de la violación y de los perjuicios derivados de la infracción, garantizando el principio del debido proceso.
3. Las multas se establecerán sobre la base de una unidad de cuenta cuyo valor se establece en PESOS CIEN MIL (\$100.000). La Autoridad de Aplicación realizará la actualización de la unidad móvil el último día hábil de cada año 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, entrando en vigencia el valor actualizado desde el momento de su publicación en el BOLETÍN OFICIAL.

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 CUATRO POR CIENTO (4 %) de la facturación total anual global del infractor en el ejercicio financiero anterior a la aplicación de la sanción”.

CAPÍTULO XI - DISPOSICIONES COMPLEMENTARIAS Y TRANSITORIAS

ARTÍCULO 77.- 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 78.- 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 de los derechos de acceso a la información pública, y promover medidas de transparencia activa”.

ARTICULO 79.- Derógase el inciso t) del artículo 24 del capítulo IV de la Ley N° 27.275 de Derecho de Acceso a la Información Pública.

ARTÍCULO 80.- Sustitúyese el artículo 29 de la Ley N° 27.275 y su modificatorio, el que dará redactado de la siguiente forma: “ARTÍCULO 29.- Consejo Federal para la Transparencia. Créase el CONSEJO FEDERAL PARA LA TRANSPARENCIA como organismo interjurisdiccional de carácter permanente, que tiene por objeto la cooperación técnica y la concertación de políticas en materia de transparencia, acceso a la información pública y protección de datos personales. El CONSEJO FEDERAL PARA LA TRANSPARENCIA tiene su sede en la AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA, de la cual recibe apoyo administrativo y técnico para su funcionamiento. El CONSEJO FEDERAL PARA LA TRANSPARENCIA está integrado por UN (1) representante de cada una de las Provincias y UN (1) representante de la Ciudad Autónoma de Buenos Aires, que deberán ser los funcionarios y/o las funcionarias de más alto rango en la materia de sus respectivas jurisdicciones. El CONSEJO FEDERAL PARA LA TRANSPARENCIA será presidido por la persona que ejerza la titularidad de la AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA, quien deberá convocar semestralmente a reuniones en donde se evaluará el grado de avance en materia de transparencia activa y acceso a la información en cada una de las jurisdicciones”.

ARTÍCULO 81.- Referencias. En todas aquellas normas en que se menciona la Ley N° 25.326 y su modificatoria, se entenderá que se hace referencia a la presente Ley.

Aquellas normas que atribuyan a la DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES el carácter de autoridad u órgano de control en materia de protección de datos personales, se entenderán referidas a la AGENCIA DE PROTECCIÓN DE LOS DATOS PERSONALES.

ARTÍCULO 82.- Derogación. Deróganse las Leyes N° 25.326 y su modificatoria N° 26.343 una vez que entre en vigencia la presente Ley, de conformidad con el artículo 82 de la presente.

ARTÍCULO 83.- Vigencia. La presente Ley entrará en vigencia transcurridos CIENTO OCHENTA (180) días corridos desde su publicación en el BOLETÍN OFICIAL, excepto el artículo 79, que comenzará a regir a partir de la referida publicación. Hasta que se



produzca la entrada en vigencia de la presente Ley, se mantendrá la vigencia de la Ley N° 25.326 y sus modificatorias.

ARTÍCULO 84.- De forma.

José Pablo Carro – Diputado de la Nación



FUNDAMENTOS

Señor Presidente:

En tiempos de intercambio globalizado de bienes y servicios, donde la información resulta un bienpreciado por sus posibilidades de análisis mediante big data y procedimientos algorítmicos, mientras se debate la pertinencia y el modo de abordaje regulatorio de la Inteligencia Artificial, a nadie escapa que la gestión, el tráfico y el uso de datos personales es la base de numerosos despliegues de negocios y posible afectación de derechos personalísimos, civiles y sociales.

En este Parlamento hemos sido consecuentes con las buenas prácticas a nivel supranacional, que basadas en protocolos de los países de la Unión Europea, dieron paso a sendos convenios suscriptos por la Argentina, lo cual nos coloca como parte de los países adecuados a las buenas prácticas de protección transfronteriza de datos. Al respecto, el 9 de noviembre de 2022, hemos sancionado en la Cámara de Diputados de la Nación la Ley 27.699, ratificando el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, conocida como Convenio 108+. La misma fue aprobada con amplísima mayoría de 206 votos afirmativos, 4 abstenciones y ninguna oposición. Hemos sido el segundo país de América Latina en ratificar el Convenio y esperamos que en un breve tiempo este instrumento multilateral de carácter vinculante reúna la cantidad ratificaciones necesarias para entrar en plena vigencia.

Sin embargo, sabemos que estamos en deuda con la armonización de la Ley nacional respecto de los principios y procedimientos que aprobamos para el tráfico transfronterizo a través de la ratificación del Convenio 108+. No podemos sostener una ley nacional anticuada, que contiene disposiciones que cayeron en desuso debido a los avances en las redes de infraestructura y alojamiento de información, mientras adherimos a las actualizaciones del tratamiento internacional de datos. Para garantizar un ambiente de negocios seguro y la tutela de los derechos de toda la población, necesitamos debatir y aprobar una nueva Ley de Datos Personales.

Los dos Poderes Ejecutivos anteriores al actual fueron conscientes de la necesidad de actualizar la Ley 25.326 sancionada en el año 2000 y aún vigente.

El proyecto de Ley 12-PE-2023 remitido al Congreso por Alberto Fernández junto con el Mensaje 87/2023, fue precedido por una ronda de consulta y audiencias públicas coordinadas por la Agencia de Acceso a la Información Pública, organismo de aplicación de las cuestiones vinculadas al tratamiento de datos personales a partir de un decreto del presidente Macri. El mencionado proyecto de ley tomó como aporte



conceptual los más recientes estándares, recomendaciones y lecciones aprendidas en nuestra región y en el mundo durante las últimas dos décadas.

El proyecto de ley que ahora presentamos reproduce buena parte del articulado de su antecedente del 2023, respetando aquel trabajo colaborativo entre agencias públicas, la academia, las organizaciones especializadas de la sociedad civil y numerosas empresas y cámaras que formaron parte del proceso consultivo y las mesas de diálogo para la elaboración de aquel anteproyecto.

A esto se suma que también hemos recibimos nuevas lecturas sobre el proyecto y aportes de organizaciones como el capítulo latinoamericano de Access Now, la Fundación Vía Libre y el Observatorio DerCom de la Carrera de Ciencias de la Comunicación de la Universidad de Buenos Aires, entre otros, a quienes agradecemos su confianza. Asimismo, hemos revisado la legislación reciente en la materia, de países como Brasil, Chile y Ecuador, lo cual nos llevó a reescribir diversos artículos en cuando a definiciones, procedimientos, enfoques de la autoridad de aplicación y su relación con los gestores privados, etc.

Debido a las experiencias de los tiempos recientes, signadas por un exceso de intervencionismo por parte de la Jefatura de Gabinete -que llegó al colmo de modificar por decreto los criterios de aplicación de la Ley de Acceso a la Información Pública y la politización del tratamiento de cuestiones muy sensibles y específicas a cargo del organismo de aplicación-, es que proponemos retrotraer la fusión decretada por Macri y disponer de una Agencia de Protección de Datos Personales diferenciada de la Agencia de Acceso a la Información Pública. Así, aspiramos a dotar de mayor autonomía, profesionalización y especialización a quienes se encargarán de cuidar a las y los argentinos respecto de cuestiones muy sensibles en la disposición de sus datos personales por terceras partes privadas o públicas.

Asimismo, actualizamos un sistema de sanciones y multas que permitirán un ejercicio real de las competencias y funciones asignadas a la autoridad de aplicación, a la vez de mayor financiamiento para estas acciones.

Como fue referido, coincidimos con los principios rectores del proyecto de ley elaborado en forma participativa entre 2022 y 2023.

El proyecto define en su Capítulo I las Disposiciones Generales, donde se incluye el objeto de la ley y una serie de definiciones que amplían el universo conceptual de la vigente Ley N° 25.326 y su modificatoria. Se mantiene en líneas generales la redacción del proyecto PEN 2023, aunque en el artículo 2° (Definiciones) se actualizan las correspondientes a Incidente de Datos Personales y Seudonimización, y en el artículo 3° en lo correspondiente a secreto de la información periodística, se



diferencia entre actividad periodística y actividad de empresas u organizaciones periodísticas o intermediarias de contenidos, entre otras actualizaciones. Se mantiene el establecimiento del ámbito de aplicación material y territorial, incluyendo al principio de extraterritorialidad que establece que la normativa se aplicará en distintos supuestos, aun cuando los Responsables de tratamiento de datos no se encuentren en territorio nacional.

En el Capítulo II 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 y los principios de finalidad; de minimización de datos; el de exactitud; de preeminencia; de responsabilidad proactiva y demostrada y el de seguridad de los datos personales. Asimismo, se determinan las bases legales para el tratamiento de datos, en el artículo 13. A lo largo de este apartado se determinan las características del consentimiento, 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 precisan en algunos párrafos redacciones que permitan prevenir usos extorsivos (artículo 8) o identificar y sancionar situaciones de engaño o fraude (artículo 14).

El Capítulo III refiere a las transferencias internacionales y en sus artículos 23, 24, 25 y 26 establece mecanismos con distinto nivel de jerarquía para realizar el flujo transfronterizo de datos personales con confianza. Se refiere a transferencias basadas en: una decisión de adecuación; mecanismos que permitan ofrecer las garantías adecuadas o excepciones, que deben darse bajo ciertas condiciones y no pueden utilizarse de manera periódica o habitual. Se incorpora el criterio general de reciprocidad en el trato entre naciones que intercambian datos.

El Capítulo IV incluye los derechos de los titulares de los datos comprendiendo, entre otros, el derecho a saber si se están tratando sus datos personales, figurando allí el derecho de acceso, el derecho de rectificación, el derecho de oposición y el derecho de supresión. El proyecto incorpora el derecho a limitación y el derecho sobre las decisiones automatizadas y la elaboración de perfiles. Atento a los desarrollos de sistemas de inteligencia artificial, se agrega a la Ley un nuevo concepto como artículo 32: “dato inferido”, definido como aquella información relativa a un individuo identificado o identificable, creada a través de razonamiento o deducción y no sólo mediante la mera observación o recolección de sus datos personales.

El Capítulo V prevé las obligaciones del Responsable y Encargado de tratamiento de datos personales. Se establecen las medidas para el cumplimiento de la responsabilidad proactiva y se incorporan la figura del Delegado de Protección de Datos, la evaluación de impacto relativa a la protección de datos y el reconocimiento de buenas prácticas adecuadas a lo establecido por la Ley, por parte de empresas u



organizaciones del sector privado. Se incorpora también la figura del Representante para aquellos Responsables y Encargados que no estén establecidos en el país y la ley resulte de aplicación conforme a los términos del artículo 4. Asimismo, se crea el Registro Nacional para la Protección de los Datos Personales (artículo 48).

El Capítulo VI regula la protección de datos de información crediticia y hace referencia a las consideraciones que se deben tener en cuenta para desarrollar de manera adecuada el tratamiento, en particular con relación al plazo de conservación y el deber de comunicar, sin perjuicio de las restantes obligaciones impuestas por la ley. Se reduce la disponibilidad de información de solvencia económica en caso de regularización de deudas a un año (tomando parte del criterio de reducción de tiempo del proyecto de ley de la diputada Gaillard, expediente 1664-D-2024).

Los Capítulos VII y VIII refieren, respectivamente, a la Autoridad de Aplicación -que se pretende jerarquizar volviendo al ordenamiento previo a la fusión dispuesta en 2016, es decir separando las Agencias de Acceso a la Información Pública de la de Protección de Datos Personales-, y la actualización de los procedimientos y sanciones a implementar en caso de constatar el incumplimiento de la ley.

El Capítulo IX regula específicamente la acción judicial de habeas data. Valoramos y sostenemos la innovación propuesta por el Proyecto de Ley PEN 2023, que consiste en la ampliación de la legitimación activa para acciones colectivas de protección de datos personales.

El Capítulo X actualiza las sanciones administrativas. En relación con las multas, el proyecto incorpora una unidad móvil sujeta a la variación del Índice de Precios al Consumidor y eleva los montos sustantivamente, con actualización semestral. Se resuelve la obsolescencia de la Ley N° 25.326, sancionada en el año 2000, que fijó multas sin posibilidad de actualización a pesar de que han transcurrido más de veinticuatro años.

El Capítulo XI establece necesarias Disposiciones Complementarias.

Por todo lo expuesto, solicitamos a nuestros pares que acompañen con su voto el presente proyecto de ley.

José Pablo Carro – Diputado de la Nación