PROYECTO DE LEY

El Senado y la Cámara de Diputados...

LEY DE PROTECCIÓN DE LOS DATOS PERSONALES

CAPÍTULO 1

DISPOSICIONES GENERALES

Artículo 1 ° .- Objeto. La presente Ley tiene por objeto la protección integral de los datos personales a fin de garantizar el ejercicio pleno de los derechos de sus titulares, de conformidad a lo establecido en el artículo 43, párrafo tercero, de la CONSTITUCIÓN NACIONAL y los Tratados de Derechos Humanos en los que la REPÚBLICA ARGENTINA sea parte.

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

- *Anonimización efectiva*: proceso mediante el cual los datos personales son transformados de forma tal que ya no puedan ser atribuidos a una persona humana identificada o identificable, perdiendo en consecuencia su carácter de datos personales. La anonimización deberá garantizar que cualquier tratamiento posterior no comprometa la exactitud ni la integridad de los datos originales y minimice al mismo tiempo el riesgo de reidentificación.
- *Autoridad de control*: órgano que debe velar por el cumplimiento de los principios y procedimientos de la presente Ley de acuerdo a lo establecido en el Capítulo 7.
- *Base de datos*: conjunto organizado de datos personales que sean objeto de tratamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso. Indistintamente se la puede denominar también archivo, registro, fichero o banco de datos.
- *Datos personales:* información de cualquier tipo referida a personas humanas determinadas o determinables, inclusive los datos biométricos. Se entenderá

por determinable la persona que pueda ser identificada mediante algún identificador o por uno o varios elementos característicos de la identidad física, fisiológica, genética (datos genéticos), psíquica, económica, cultural o social de dicha persona. No será considerada persona determinable cuando, para lograr su identificación, se requiera la aplicación de medidas o plazos desproporcionados o inviables. Se entenderá por 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. Se entenderá por datos genéticos los relativos a las características genéticas heredadas o adquiridas de una persona humana que proporcionen una información sobre su fisiología o salud, obtenidos en particular del análisis de una muestra biológica.

- *Datos sensibles*: datos personales que afectan la esfera íntima de su titular con potencialidad de originar una discriminación ilícita o arbitraria, en particular, los que revelan origen racial o étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, participación o afiliación en una organización sindical o política, información referente a la salud, preferencia o vida sexual.
- *Disociación de datos*: el procedimiento que se aplica sobre los datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable. No será considerada persona determinable cuando el procedimiento que deba aplicarse para lograr su identificación requiera la aplicación de medidas o plazos desproporcionados o inviables.
- *Encargado del tratamiento*: persona humana o jurídica, pública o privada, que trate datos personales por cuenta del responsable del tratamiento.
- *Entidades crediticias*: comprende a las entidades que proveen información de situación crediticia al BANCO CENTRAL DE LA REPÚBLICA ARGENTINA.
- *Fuente de acceso público irrestricto*: la que contiene información destinada a ser difundida al público, de libre acceso e intercambio por razones de interés general, accesible ya sea en forma gratuita o mediante una contraprestación.

- *Fuente de acceso público restricto*: la que contiene información que no está sujeta a confidencialidad ni tampoco está destinada a ser difundida irrestrictamente al público y cuyo acceso a terceros resulta generalmente condicionado al cumplimiento de ciertos requisitos.

- *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.

- *Incidente de seguridad de datos personales*: hecho ocurrido en cualquier fase del tratamiento que implique la pérdida o destrucción no autorizada, el robo, extravío o copia no autorizada, el uso, acceso o tratamiento de datos no autorizado, o el daño, alteración o modificación no autorizada.

- *Responsable del tratamiento*: persona humana o jurídica, pública o privada, titular de la base de datos, que decide sobre el tratamiento de datos, sus finalidades y medios.

- *Tercero*: la persona humana o jurídica, pública o privada, distinta del titular de los datos, del responsable del tratamiento, del encargado del tratamiento o de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado

- *Titular de los datos:* la persona humana cuyos datos sean objeto del tratamiento al que se refiere la presente Ley.

- *Transferencia internacional:* la transmisión de datos personales fuera del territorio nacional.

- *Tratamiento de datos*: cualquier operación o procedimiento organizado, electrónico o no, que permita la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo o destrucción y, en general, el procesamiento de datos personales, así como también su cesión a través de comunicaciones, consultas, interconexiones o transferencias.

Artículo 3 ° .- Excepciones a la aplicación de la 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.
La aplicación de la presente Ley en ningún caso podrá afectar el secreto de las fuentes de información periodísticas. Tampoco podrá afectar al tratamiento de datos que realicen los medios de comunicación en el ejercicio de la libertad de expresión.

Artículo 4 ° .- Ámbito de aplicación. Las normas de la presente Ley serán de aplicación cuando:
a) El responsable del tratamiento se encuentre establecido en el territorio nacional, aun cuando el tratamiento de datos tenga lugar fuera de dicho territorio;

b) El responsable del tratamiento no se encuentre establecido en el territorio nacional, sino en un lugar en que se aplica la legislación nacional en virtud del derecho internacional;

c) El tratamiento de datos de titulares que residan en la REPÚBLICA ARGENTINA sea realizado por un responsable del tratamiento que no se encuentre establecido en el territorio nacional y las actividades de dicho tratamiento se encuentren relacionadas con la oferta de bienes o servicios a dichos titulares de los datos en la REPÚBLICA ARGENTINA, o con el seguimiento de sus actos, comportamientos o intereses.

CAPÍTULO 2
PRINCIPIOS RELATIVOS AL TRATAMIENTO DE DATOS

Artículo 5º.- Principio de licitud, lealtad y transparencia. Los datos personales deben ser tratados de manera lícita, leal y transparente. El tratamiento se considera leal cuando el responsable se abstenga de tratar los datos personales a través de medios engañosos o fraudulentos.

Artículo 6º.- Principio de finalidad. Los datos personales deben ser recogidos con fines determinados, explícitos y legítimos, y no deben ser tratados de manera incompatible con dichos fines.
No se considerarán incompatibles con los fines iniciales tanto el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos, como tampoco el tratamiento de datos con fines que pudieron ser, de acuerdo al contexto, razonablemente presumidos por el titular de los datos.

Artículo 7º.- 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.

Artículo 8º.- Principio de exactitud. Los datos personales deben ser tratados de modo que sean exactos y completos. Si fuera necesario adecuarlos, se adoptarán todas las medidas razonables para que se supriman o rectifiquen. Quedan excluidos de esta obligación los datos que hayan sido previamente anonimizados de forma efectiva, en tanto que no pueden ser asociados directa o indirectamente con una persona identificada o identificable, y por tanto no constituyen datos personales conforme a esta ley.

Artículo 9º.- Plazo de conservación. Los datos personales no deben ser mantenidos más allá del tiempo estrictamente necesario para el cumplimiento de la finalidad del tratamiento. Los datos personales pueden conservarse durante períodos más largos siempre que se trate exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone la presente Ley a fin de proteger los derechos del titular de los datos.

Artículo 10 ° .- Principio de responsabilidad proactiva. El responsable o encargado del tratamiento debe adoptar las medidas técnicas y organizativas apropiadas a fin de garantizar un tratamiento adecuado de los datos personales y el cumplimiento de las obligaciones dispuestas por la presente Ley, y que le permitan demostrar a la autoridad de control su efectiva implementación.

Artículo 11 ° .- Licitud del tratamiento de datos. El tratamiento de datos es lícito sólo si se cumple al menos UNA (1) de las siguientes condiciones:

a) El titular de los datos dio su consentimiento para el tratamiento de sus datos para uno o varios fines específicos conforme lo dispuesto en los artículos 12, 13 y 14;

b) El tratamiento de datos se realice sobre datos que figuren en fuentes de acceso público irrestricto;

c) El tratamiento de datos se realice en ejercicio de funciones propias de los poderes del Estado y sean necesarios para el cumplimiento estricto de sus competencias;

d) El tratamiento de datos sea necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

e) El tratamiento de datos derive de una relación jurídica entre el titular de los datos y el responsable del tratamiento, y resulte necesario para su desarrollo o cumplimiento;

f) El tratamiento de datos resulte necesario para salvaguardar el interés vital del titular de los datos o de terceros, y el titular de los datos esté física o jurídicamente incapacitado para dar su consentimiento;

g) El tratamiento de datos sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos del titular de los datos, en particular cuando el titular sea un niño, niña o adolescente.

h) Los datos han sido efectivamente anonimizados.

Lo dispuesto en el inciso g) no será de aplicación al tratamiento de datos realizado por las autoridades públicas en el ejercicio de sus funciones.

Artículo 12 ° .- Consentimiento. El tratamiento de datos, en cualquiera de sus formas, requiere del consentimiento libre e informado de su titular para una o varias finalidades específicas.
El consentimiento puede ser obtenido de forma expresa o tácita.
La forma del consentimiento depende de las circunstancias, el tipo de dato personal y las expectativas razonables del titular de los datos.
El consentimiento expreso, de acuerdo a las circunstancias particulares del tratamiento de datos del que se trate, puede ser obtenido por escrito, verbalmente, por medios electrónicos, así como por cualquier forma similar que la tecnología permita brindar.
Para el tratamiento de datos sensibles se requiere el consentimiento expreso, salvo las excepciones establecidas por ley.
El consentimiento tácito es admitido cuando surja de manera manifiesta del contexto del tratamiento de datos y la conducta del titular de los datos sea suficiente para demostrar la existencia de su autorización. Es admisible únicamente cuando los datos requeridos sean necesarios para la finalidad que motiva la recolección y se haya puesto a disposición del titular de los datos la información prevista en el artículo 15, sin que éste manifieste su oposición. El tratamiento de datos ulterior debe ser compatible con las finalidades manifiestas que surgen del contexto que originó la recolección. En ningún caso procede para el tratamiento de datos sensibles.
En todos los casos, el responsable del tratamiento tiene la carga de demostrar que el titular de los datos consintió el uso de sus datos personales.

Artículo 13 ° .- Revocación del consentimiento. El consentimiento puede ser revocado en cualquier momento. Dicha revocación no tiene efectos retroactivos. El responsable del tratamiento está obligado a facilitar la revocación mediante mecanismos sencillos, gratuitos y, al menos, de la misma forma por la que obtuvo el consentimiento.

Artículo 14 ° .- Excepciones al consentimiento previo. No es necesario el consentimiento para el tratamiento de datos cuando se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento, domicilio y correo electrónico, con la salvedad dispuesta en el párrafo 7 del artículo 60 de la presente.

Artículo 15 ° .- Información al titular de los datos. El responsable del tratamiento debe brindar al titular de los datos, antes de la recolección, al menos, la siguiente información:

a) Las finalidades del tratamiento de datos a las que se destinarán los datos personales recolectados

b) La identidad y los datos de contacto del responsable del tratamiento;

c) Los medios para ejercer los derechos previstos en esta Ley;

d) En su caso, las cesiones o transferencias internacionales de datos que se efectúen o se prevea efectuar;

e) 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;

f) El derecho del titular de los datos a revocar el consentimiento;

g) El derecho a presentar una denuncia, a iniciar el trámite de protección de datos personales ante la autoridad de control, o a ejercer la acción de habeas data en caso de que el responsable o el encargado del tratamiento incumpla con la presente Ley.

Artículo 16 ° .- Tratamiento de datos sensibles. Se prohíbe el tratamiento de datos sensibles, excepto cuando:

a) El titular de los datos haya dado su consentimiento expreso a dicho tratamiento, salvo en los casos en que por ley no sea requerido el otorgamiento de dicha autorización;

b) Sea necesario para salvaguardar el interés vital del titular de los datos y éste se encuentre física o legalmente incapacitado para prestar el consentimiento y sus representantes legales no lo puedan realizar en tiempo oportuno;

c) Sea efectuado por establecimientos sanitarios públicos o privados o por profesionales vinculados a la ciencia de la salud en el marco de un tratamiento médico específico de acuerdo a lo establecido por la Ley Derechos del Paciente, Historia Clínica y Consentimiento Informado Nº 26.529 y sus modificatorias;

d) Se realice en el marco de las actividades legítimas que realice 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 a sus miembros o beneficiarios o a las personas que mantengan un contacto regular por razón de su objeto principal;

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

f) Tenga una finalidad histórica, estadística o científica. En estos DOS (2) últimos casos, debe adoptarse un procedimiento de disociación de datos;

g) Se refiera a datos personales que el interesado haya hecho manifiestamente públicos;

h) Sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del titular de los datos en el ámbito del Derecho Laboral y de la Seguridad y Protección Social;

i) Sea necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios;

j) Se realiza en el marco de asistencia humanitaria en casos de desastres naturales.

Artículo 17°.- Tratamiento de antecedentes penales y contravencionales. El tratamiento de datos relativos a antecedentes penales o contravencionales con el objeto de brindar informes a terceros sólo puede ser realizado por parte de las autoridades públicas competentes o bajo su supervisión.
El empleador que conserve un certificado, documento o información de antecedentes penales o contravencionales de sus empleados no puede cederlo a terceros, salvo con el consentimiento expreso del titular de los datos.

Artículo 18 ° .- Tratamiento de datos de niños, niñas y adolescentes. En el tratamiento de datos personales de un niño, niña o adolescente, se debe privilegiar la protección del interés superior de éstos, conforme a la CONVENCIÓN SOBRE LOS DERECHOS DEL NIÑO y demás instrumentos internacionales que busquen su bienestar y protección integral.
Es válido el consentimiento de un niño, niña o adolescente cuando se aplique al tratamiento de datos vinculados a la utilización de servicios de la sociedad de la información específicamente diseñados o aptos para ellos. En estos casos, el consentimiento es lícito si el niño, niña o adolescente tiene como mínimo TRECE (13) años. Si ellos son menores de TRECE (13) años, tal tratamiento únicamente se considera lícito si el consentimiento fue otorgado por el titular de la responsabilidad parental o tutela sobre el niño, y sólo en la medida en que se dio o autorizó.
El responsable del tratamiento debe realizar esfuerzos razonables para verificar, en tales casos, que el consentimiento haya sido otorgado por el titular de la responsabilidad parental o tutela sobre el niño, niña o adolescente, teniendo en cuenta sus posibilidades para hacerlo.

Artículo 19 ° .- Principio de seguridad de los datos personales. El responsable del tratamiento y, en su caso, el encargado, deben adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, 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.
El responsable del tratamiento debe adoptar las medidas de seguridad aplicables a los datos personales que trate, considerando, 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 los titulares de los datos;

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

Artículo 20 ° .- Notificación de incidentes de seguridad. En caso de que ocurra un incidente de seguridad de datos personales, el responsable del tratamiento debe notificarlo a la autoridad de control sin dilación indebida y, de ser posible, a más tardar SETENTA Y DOS (72) horas después de que haya tenido constancia del incidente, a menos que sea improbable que dicho incidente de seguridad constituya un riesgo para los derechos de los titulares de los datos.
Si la notificación a la autoridad de control no tiene lugar en el plazo de SETENTA Y DOS (72) horas, deberá ir acompañada de indicación de los motivos de la dilación.
De igual manera, el responsable del tratamiento también debe informar al titular de los datos sobre el incidente de seguridad ocurrido, en un lenguaje claro y sencillo, cuando sea probable que entrañe altos riesgos a sus derechos.
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 al titular de los datos acerca de las medidas que éste pueda adoptar para proteger sus intereses;

e) Los medios a disposición del titular de los datos para obtener mayor información al respecto.

El responsable del tratamiento debe documentar todo incidente de seguridad que ponga en alto riesgo los derechos de los titulares de los datos personales 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 éste y sus efectos y las medidas correctivas implementadas de forma inmediata y definitiva.

Artículo 21 ° .- Deber de confidencialidad. El responsable del tratamiento, el encargado y las demás personas que intervengan en cualquier fase del tratamiento de datos están obligados a la confidencialidad respecto de los datos personales. Tal obligación subsiste aun después de finalizada su relación con el titular de los datos, el responsable o el encargado del tratamiento, según corresponda.

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

Artículo 22 ° .- Cesión. Cuando el tratamiento de datos consiste en una cesión, el responsable del tratamiento a quien se ceden los datos personales queda sujeto a las mismas obligaciones legales y reglamentarias que el responsable cedente. Ambos responden por la observancia de aquéllas ante la autoridad de control y el titular de los datos de que se trate. En cualquier caso, podrán ser eximidos total o parcialmente de responsabilidad si demuestran que no se les puede imputar el hecho que ha producido el daño.

Artículo 23 ° .- Transferencia internacional. Toda transferencia internacional de datos personales es lícita si se cumple al menos UNA (1) de las siguientes condiciones:

a) Cuente con el consentimiento expreso del titular de los datos;

b) El país u organismo internacional o supranacional receptor proporcione un nivel de protección adecuado;

c) Se encuentre prevista en una ley o tratado en los que la REPÚBLICA ARGENTINA sea parte;

d) Sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios;

e) Sea efectuada a cualquier sociedad del mismo grupo económico del responsable del tratamiento, en tanto los datos personales sean utilizados para finalidades que no sean incompatibles con las que originaron su recolección;

f) Sea necesaria en virtud de un contrato celebrado o por celebrar en interés inequívoco del titular de los datos, por el responsable del tratamiento y un tercero;

g) Sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia;

h) Sea necesaria para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial;

i) Sea necesaria para el mantenimiento o cumplimiento de una relación jurídica entre el responsable del tratamiento y el titular de los datos;

j) Sea efectuada en los casos de colaboración judicial internacional;

k) Sea requerida para concretar transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable;

l) Tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo, el lavado de activos, los delitos informáticos y el narcotráfico;

m) El responsable del tratamiento transferente y el destinatario adopten mecanismos de autorregulación vinculantes, siempre y cuando éstos sean acordes a las disposiciones previstas en esta Ley;

n) Se realice en el marco de cláusulas contractuales que contengan mecanismos de protección de los datos personales acordes con las disposiciones previstas en la presente Ley.
El receptor de los datos personales asume las mismas obligaciones que corresponden al responsable del tratamiento que transfirió los datos personales.

Artículo 24 ° .- Carácter adecuado del país u organismo receptor. Se entiende que un país u organismo internacional o supranacional proporciona un nivel adecuado de protección cuando dicha tutela se deriva directamente del ordenamiento jurídico vigente.
El nivel de protección proporcionado por un país u organismo internacional o supranacional será evaluado por la autoridad de control, a pedido de parte interesada o de oficio y atendiendo a todas las circunstancias que concurran en una transferencia internacional; en particular, las normas de derecho, generales o especiales, vigentes en el país u organismo internacional o supranacional de que se trate, así como las normas profesionales, códigos de conducta y las medidas de seguridad que resulten aplicables.

Artículo 25 ° .- Prueba del cumplimiento de las obligaciones en materia de transferencias internacionales.
A efectos de demostrar que la transferencia internacional se ha realizado conforme a lo que establece la presente Ley, la carga de la prueba recae, en todos los casos, en el responsable del tratamiento que transfiere.

Artículo 26 ° .- Servicio de tratamiento de datos personales por medios tecnológicos tercerizados. El servicio de tratamiento de datos personales por medios tecnológicos tercerizados está permitido cuando se garantice el cumplimiento de los principios y obligaciones establecidos en la presente Ley.
El responsable del tratamiento debe realizar esfuerzos razonables para elegir un proveedor de servicios que garantice el cumplimiento de la presente Ley. El

responsable del tratamiento responderá ante el titular de los datos y ante la autoridad de control por incumplimientos del proveedor.

En especial, el responsable del tratamiento debe realizar esfuerzos razonables para controlar que el proveedor del servicio de tratamiento de datos personales por medios tecnológicos tercerizados:

a) Cuente con una política de protección de datos personales o condiciones de servicio que no sean incompatibles con las disposiciones previstas en la presente Ley, y que su aplicación sea efectiva, y además verificar que se prevean mecanismos para notificar los cambios que se produzcan sobre la política de protección de datos personales o condiciones de servicio;

b) Informe los tipos de subcontrataciones que involucren los datos personales objeto del tratamiento sobre el que se presta el servicio, notificando al responsable del tratamiento de cualquier cambio que se produzca;

c) No incluya condiciones en la prestación del servicio que lo autoricen o permitan asumir la titularidad sobre las bases de datos tratados bajo esta modalidad.

CAPÍTULO 3
DERECHOS DE LOS TITULARES DE LOS DATOS

Artículo 27 ° .- Derecho de acceso. El titular de los datos, previa acreditación de su identidad, tiene el derecho de solicitar y obtener el acceso a sus datos personales que sean objeto del tratamiento.

Artículo 28°. - Contenido de la información. La información debe ser suministrada en forma clara, exenta de codificaciones y, en su caso, acompañada de una explicación de los términos que se utilicen, en lenguaje accesible al conocimiento medio de la población, y debe versar sobre:

a) Las finalidades del tratamiento de datos;

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

c) Los destinatarios o las categorías de destinatarios a los que se cedieron o se prevean ceder los datos personales, en particular cuando se trate de una transferencia internacional;

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

e) La existencia del derecho a solicitar del responsable del tratamiento la rectificación, supresión de datos personales o a oponerse a dicho tratamiento, salvo que se trate de datos efectivamente anonimizados;

f) El derecho a iniciar un trámite de protección de datos personales ante la autoridad de control;

g) Cuando los datos personales no se hayan obtenido del titular de los datos, cualquier información disponible sobre su origen;

h) La existencia de decisiones automatizadas, incluida la elaboración de perfiles a que se refiere el artículo 32 y, al menos en tales casos, información significativa sobre la lógica aplicada, sin que ello afecte derechos intelectuales del responsable del tratamiento.

En ningún caso el informe puede revelar datos pertenecientes a terceros, aun cuando se vinculen con el titular de los datos.

La información, a opción del titular de los datos, puede suministrarse por escrito, por medios electrónicos, telefónicos, de imagen, u otro idóneo a tal fin.

Artículo 29 ° .- Derecho de rectificación. El titular de los datos tiene el derecho a obtener del responsable del tratamiento la rectificación de sus datos personales, cuando éstos resulten ser inexactos, incompletos o no se encuentren actualizados.

En el supuesto de cesión o transferencia internacional de datos erróneos o desactualizados, el responsable del tratamiento debe notificar la rectificación al cesionario dentro del Quinto (5°) día hábil de haber tomado conocimiento efectivo del error o la desactualización.

Durante el proceso de verificación y rectificación del error o falsedad de la información que se trate, el responsable del tratamiento debe bloquear el dato,

o bien consignar, al proveer información relativa a éste, la circunstancia de que se encuentra sometido a revisión.
Se exceptúa de este derecho la información relativa a datos previamente anonimizados, en la medida en que estos ya no puedan asociarse directa ni indirectamente con una persona identificada o identificable, y por tanto, no sean considerados datos personales conforme a la presente ley.

Artículo 30 ° .- Derecho de oposición. El titular de los datos puede oponerse al tratamiento de sus datos, o de una finalidad específica de éste, cuando no haya prestado consentimiento. El responsable del tratamiento debe dejar de tratar los datos personales objeto de oposición, salvo que existan motivos legítimos para el tratamiento que prevalezcan sobre los derechos del titular de los datos.

Artículo 31 ° .- Derecho de supresión. El titular de los datos tiene derecho a solicitar la supresión de sus datos personales de las bases de datos del responsable del tratamiento cuando el tratamiento no tenga un fin público, a fin de que los datos ya no estén en su posesión y dejen de ser tratados por este último.

La supresión procede cuando:
a) Los datos personales ya no sean necesarios en relación con los fines para los que fueron recolectados;

b) El titular de los datos revoque el consentimiento en que se basa el tratamiento de datos y éste no se ampare en otro fundamento jurídico;

c) El titular de los datos haya ejercido su derecho de oposición conforme al artículo 30, y no prevalezcan 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.

La supresión no procederá cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, prevalezcan razones de interés público para el tratamiento de datos cuestionado, o los datos personales deban ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las contractuales entre el responsable o encargado del tratamiento y el titular de los datos.
La supresión tampoco procede cuando el tratamiento de datos sea necesario para ejercer el derecho a la libertad de expresión e información.

Artículo 32 ° .- Valoraciones personales automatizadas. El titular de los datos tiene derecho a oponerse a ser objeto de una decisión basada únicamente en el tratamiento automatizado de datos, incluida la elaboración de perfiles, que le produzca efectos jurídicos perniciosos o lo afecte significativamente de forma negativa.
El titular de los datos no podrá ejercer este derecho si la decisión:
a) Es necesaria para la celebración o la ejecución de un contrato entre el titular de los datos y el responsable del tratamiento;

b) Está autorizada por Ley;

c) Se basa en su consentimiento expreso.
En los casos a que se refieren los incisos a) y c), el responsable del tratamiento debe adoptar las medidas adecuadas para salvaguardar los derechos del titular de los datos; como mínimo, el derecho a obtener intervención humana por parte del responsable del tratamiento, a expresar su punto de vista y a impugnar la decisión.

Artículo 33 ° .- Derecho a la portabilidad de datos personales. Si se brindan servicios en forma electrónica que incluyan el tratamiento de datos personales, el titular de los datos tiene derecho a obtener del responsable del tratamiento una copia de los datos personales objeto de tratamiento en un formato estructurado y comúnmente utilizado que le permita su ulterior utilización. El titular de los datos puede solicitar que sus datos personales se transfieran

directamente de responsable a responsable cuando sea técnicamente posible. Este derecho no procederá cuando:

a) Su ejercicio imponga una carga financiera o técnica excesiva o irrazonable sobre el responsable o encargado del tratamiento;

b) Vulnere la privacidad de otro titular de los datos;

c) Vulnere las obligaciones legales del responsable o encargado del tratamiento;

d) impida que el responsable del tratamiento proteja sus derechos, su seguridad o sus bienes, o los derechos, seguridad y bienes del encargado del tratamiento, o del titular de los datos o de un tercero.

Artículo 34 ° .- Ejercicio de los derechos. El ejercicio de cualquiera de los derechos del titular de los datos no es requisito previo, ni impide el ejercicio de otro.

El responsable del tratamiento debe responder y, en su caso, satisfacer los derechos del titular de los datos dentro de los DIEZ (10) días hábiles de haber sido intimado fehacientemente.

Vencido el plazo sin que se satisfaga el pedido, o si a juicio del titular de los datos, la respuesta se estimara insuficiente, quedará expedito el trámite de protección de los datos personales ante la autoridad de control en los términos del artículo 72 o, a elección del titular de los datos, podrá interponer la acción de hábeas data prevista en el artículo 78 de la presente Ley. En caso de optar por la acción de habeas data, o de haberla iniciado con anterioridad, no podrá iniciar el trámite de protección ante la autoridad de control.

El ejercicio de los derechos previstos en los artículos 27, 29, 30, 31, 32 y 33 en el caso de titulares de los datos de personas fallecidas les corresponde a sus sucesores universales.

El responsable del tratamiento debe establecer medios y procedimientos sencillos, expeditos, accesibles y gratuitos que permitan al titular de los datos ejercer los derechos previstos en esta Ley.

El derecho de acceso a que se refiere el artículo 27 sólo puede ser ejercido en forma gratuita a intervalos no inferiores a SEIS (6) meses, salvo que se acredite la existencia de nuevas razones que justifiquen el pedido antes del vencimiento del plazo.

Artículo 35 ° .- Abuso de derecho. 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, el que excede los límites impuestos por la buena fe o el que imponga sobre el obligado una carga técnica o financiera irrazonable.

Artículo 36 ° .- Excepciones al ejercicio de los derechos. Los responsables del tratamiento de bases de datos públicas pueden, mediante decisión fundada, denegar los derechos enumerados en los artículos 27, 29, 30, 31, 32 y 33 en función de la protección de la defensa de la Nación, del orden y la seguridad públicos, o de la protección de los derechos e intereses de terceros.
La información sobre datos personales también puede ser denegada por los responsables del tratamiento de bases de datos públicas, cuando de tal modo se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de delitos penales y la verificación de infracciones administrativas. La resolución que así lo disponga debe ser fundada y notificada al titular de los datos. En cualquier caso, el responsable del tratamiento debe brindar acceso a los datos en cuestión en la oportunidad en que el titular de los datos demuestre que son necesarios para ejercer su derecho de defensa.

CAPÍTULO 4
OBLIGACIONES DE LOS RESPONSABLES Y ENCARGADOS DEL TRATAMIENTO

Artículo 37 ° .- Medidas para el cumplimiento de la responsabilidad proactiva. Las medidas adoptadas para el cumplimiento de las disposiciones de la presente Ley deben ser 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 su titular.

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 los titulares de los datos;

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

Las medidas deben ser aplicadas de modo que permitan su demostración ante el requerimiento de la autoridad de control.

Se debe adoptar una política de privacidad o adherirse a mecanismos de autorregulación vinculantes, que serán valorados por la autoridad de control para verificar el cumplimiento de las obligaciones por parte del responsable del tratamiento.

Artículo 38 ° .- Protección de datos desde el diseño y por defecto. El responsable del tratamiento debe aplicar medidas tecnológicas y organizativas apropiadas tanto con anterioridad como durante el tratamiento de datos a fin de cumplir los principios y los derechos de los titulares de los datos establecidos en la presente Ley. Las medidas deben ser adoptadas teniendo en cuenta el estado de la tecnología, los costos de la implementación y la naturaleza, ámbito, contexto y fines del tratamiento de datos, así como los riesgos que entraña el tratamiento para el derecho a la protección de los datos de sus titulares.

El responsable del tratamiento debe aplicar las medidas tecnológicas y organizativas apropiadas con miras a garantizar que, por defecto, sólo sean

objeto de tratamiento de datos aquellos datos personales que sean necesarios para cada uno de los fines del tratamiento. Esta obligación se aplica a la cantidad y calidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas deben garantizar en particular que, por defecto, los datos personales no sean accesibles, sin la intervención del titular de los datos, a un número indeterminado de personas humanas.

Artículo 39 ° .- Tratamiento de datos por cuenta de terceros. La prestación de servicios de tratamiento de datos por cuenta de terceros entre un responsable y un encargado del tratamiento debe quedar formalizada mediante un contrato y no requiere del consentimiento del titular de los datos. El encargado del tratamiento se encuentra limitado a llevar a cabo sólo aquellos tratamientos de datos encomendados por el responsable del tratamiento. Los datos personales objeto de tratamiento no pueden aplicarse o utilizarse con un fin distinto al que figure en el contrato ni ser cedidos a otras personas, ni aun para su conservación, salvo autorización expresa del responsable del tratamiento.
Una vez cumplida la prestación contractual, los datos personales tratados deben ser destruidos, salvo que medie autorización expresa del responsable del tratamiento cuando razonablemente se pueda presumir la posibilidad de ulteriores encargos, en cuyo caso sólo podrán conservarse por un máximo de DOS (2) años.
El encargado puede suscribir un contrato para subcontratar servicios que impliquen el tratamiento de datos solamente cuando exista una autorización expresa del responsable del tratamiento. En estos casos el subcontratado asume el carácter de encargado 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, asumirá la calidad de responsable del 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 titulares de los datos y las obligaciones y responsabilidades del responsable y encargado del tratamiento.

Artículo 40 ° .- Evaluación de impacto relativa a la protección de datos personales. Cuando el responsable del tratamiento prevea realizar algún tipo de tratamiento de datos que por su naturaleza, alcance, contexto o finalidades, sea probable que entrañe un alto riesgo de afectación a los derechos de los titulares de los datos amparados en la presente Ley, deberá realizar, de manera previa a la implementación del tratamiento, una evaluación del impacto relativa a la protección de los datos personales.
La evaluación de impacto relativa a la protección de los datos es obligatoria en los siguientes casos, sin perjuicio de otros que establezca la autoridad de control:
a) Evaluación sistemática y exhaustiva de aspectos personales de personas humanas que se base en un tratamiento de datos automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas humanas o que les afecten significativamente de modo similar;

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

Artículo 41 ° .- 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, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del 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 los titulares de los datos a que se refiere el inciso a);

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 42 ° .- Informe previo. El responsable del tratamiento debe informar a la autoridad de control antes de proceder al tratamiento de datos cuando una evaluación de impacto relativa a la protección de los datos muestre que el tratamiento de datos entrañaría un alto riesgo.
El informe a la autoridad de control debe incluir, como mínimo, la siguiente información:
a) Las responsabilidades respectivas del responsable del tratamiento y los encargados del 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 proteger los datos personales de sus titulares de conformidad con la presente Ley;

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.
Cuando la autoridad de control considere que el tratamiento de datos previsto pueda infringir la presente Ley, iniciará el procedimiento de verificación de oficio establecido en el artículo 66.

Artículo 43 ° .- Delegado de Protección de Datos. Los responsables y encargados del tratamiento deben designar un Delegado de Protección de Datos en cualquiera de los siguientes supuestos:
a) Cuando revistan el carácter de autoridades u organismos públicos;

b) Se realice tratamiento de datos sensibles como parte de la actividad principal del responsable o encargado del tratamiento;

c) Se realice tratamiento de datos a gran escala, conforme a los criterios que establezca la autoridad de control mediante reglamentación.

Cuando los responsables y encargados del tratamiento no se encuentren obligados a la designación de un Delegado de Protección de Datos de acuerdo a lo previsto en este artículo, pero decidan designar de manera voluntaria o por orden expresa de la autoridad de control, el Delegado de Protección de Datos designado tendrá las funciones previstas en el artículo 44.

Cuando 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 establecimiento.

La designación del 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.

Las funciones del Delegado de Protección de Datos pueden ser desempeñadas por un empleado del responsable o encargado del tratamiento o en el marco de un contrato de locación de servicios. El Delegado de Protección de Datos puede ejercer otras funciones siempre que no den lugar a conflictos de intereses.

En cualquier caso, el delegado debe ejercer sus funciones sin recibir instrucciones y sólo responde ante el más alto nivel jerárquico de la organización.

Artículo 44 ° .- 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 del tratamiento, así como a sus empleados, de las obligaciones que tienen, derivadas de la normativa de protección de datos;

b) Promover y participar en el diseño y aplicación de una política de protección de datos que contemple los tratamientos de datos que realice el responsable o encargado del tratamiento;

c) Supervisar el cumplimiento de la presente Ley y de la política de protección de datos de un organismo público, empresa o entidad privada;

d) Asignar responsabilidades, concientizar y 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 los titulares de los datos, y supervisar luego su aplicación;

f) Cooperar y actuar como referente ante la autoridad de control para cualquier consulta sobre el tratamiento de datos efectuado por el responsable o encargado del tratamiento.

Artículo 45 ° .- Mecanismos de autorregulación vinculantes. La autoridad de control alentará la elaboración de mecanismos de autorregulación vinculantes que tengan por objeto 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 del titular de los datos.

Los mecanismos de autorregulación vinculantes se pueden traducir en códigos de conducta, de buenas prácticas, normas corporativas vinculantes, sellos de confianza, certificaciones u otros mecanismos que coadyuven a contribuir a los objetivos señalados.

Los responsables o encargados del tratamiento pueden adherirse, de manera voluntaria, a mecanismos de autorregulación vinculantes.

Las asociaciones u otras entidades representativas de categorías de responsables o encargados del tratamiento podrán adoptar mecanismos de autorregulación vinculantes que resulten obligatorios para todos sus miembros.

Los mecanismos de autorregulación vinculantes serán presentados a la

homologación de la autoridad de control, la cual dictaminará si los mecanismos se adecuan a las disposiciones de la presente Ley y, en su caso, los aprobará o indicará las correcciones que estime necesarias para su aprobación.
Los mecanismos de autorregulación vinculantes que resulten aprobados serán registrados y dados a publicidad por la autoridad de control.

CAPÍTULO 5
REGISTRO NACIONAL "NO LLAME"

Artículo 46 ° .- REGISTRO NACIONAL "No Llame". Créase, en el ámbito de la autoridad de control de la presente Ley, el Registro Nacional "No Llame".

Artículo 47 ° .- Objeto y principio rector. El objeto del registro establecido por el artículo 46 es proteger los datos personales de los titulares o usuarios autorizados de los servicios de telefonía, en cualquiera de sus modalidades, del contacto, publicidad, oferta, venta y regalo de bienes o servicios no solicitados. Las situaciones contempladas y reguladas en el presente Capítulo se deben interpretar en todos los casos teniendo en cuenta el requerimiento del titular o usuario.

Artículo 48 ° .- Servicios de telefonía. A los efectos del presente Capítulo, se entenderá por "servicios de telefonía" los servicios de telefonía básica, telefonía móvil, servicios de radiocomunicaciones móvil celular, de comunicaciones móviles y de voz IP, así como cualquier otro tipo de servicio similar que la tecnología permita brindar en el futuro.

Artículo 49 ° .- Inscripción. Puede inscribirse en el Registro Nacional "No Llame" toda persona humana titular o usuaria autorizada del servicio de telefonía en cualquiera de sus modalidades que manifieste su voluntad de no ser contactada por quien publicite, oferte, venda o regale bienes o servicios, sin perjuicio de lo dispuesto en el artículo 61 de la presente Ley.

Artículo 50 ° .- Gratuidad y simplicidad. La inscripción y baja en el Registro Nacional "No Llame" es gratuita y debe ser implementada por medios eficaces y sencillos. Los trámites de inscripción y baja sólo pueden ser realizados por el titular o usuario de la línea telefónica.
La baja puede ser solicitada en cualquier momento y debe tener efectos inmediatos.

Artículo 51 ° .- Sujetos obligados e inscripción. Quienes publiciten, oferten, vendan o regalen bienes o servicios mediante recursos propios o a través de empresas tercerizadas o subcontratadas, utilizando como medio de contacto los servicios de telefonía en cualquiera de sus modalidades, son considerados responsables del tratamiento de datos y sujetos obligados al cumplimiento de lo previsto en el presente Capítulo.
También son sujetos obligados aquellos que por cuenta de terceros realicen el contacto telefónico, sin perjuicio de la responsabilidad de quien resulte el contratante de la campaña o beneficiario directo de ésta, resultando aplicables, en el caso de corresponder, las previsiones del artículo 22.
Los sujetos obligados que contratan campañas en el exterior con efectos en el país deben adoptar las medidas apropiadas para que quien lleve a cabo la campaña publicitaria desde el extranjero dé cumplimiento a las disposiciones de la presente. Cualquier incumplimiento será atribuido al contratante o beneficiario directo de la campaña.
Es responsable solidario el titular de la línea telefónica de la que provenga el contacto de publicidad, oferta, venta y regalo de bienes o servicios no solicitados si se tratara de persona distinta a las indicadas en los párrafos precedentes. El titular de la línea telefónica podrá ser eximido total o parcialmente de responsabilidad si demuestra que no se le puede imputar el hecho que ha producido el daño.
Los sujetos obligados no pueden dirigirse a ninguno de los inscriptos en el Registro Nacional "No Llame".
Quienes realicen efectivamente el contacto telefónico deben:

a) Consultar las inscripciones vigentes que figuren en el Registro Nacional "No Llame" con una periodicidad de no más de TREINTA (30) días, en la forma que disponga la autoridad de control;

b) Estar inscriptos en un registro habilitado por la autoridad de control para la consulta en el Registro Nacional "No Llame" prevista en el inciso a); la autoridad de control establecerá el procedimiento para esa inscripción.
En caso de duda, debe interpretarse que no corresponde el contacto telefónico con quien se hubiera inscripto en el Registro Nacional "No Llame".

Artículo 52 ° .- Excepciones. Quedan exceptuadas de las disposiciones del presente Capítulo:
a) Las llamadas de quienes tienen una relación contractual vigente, siempre que se refieran al bien o servicio específico objeto del vínculo contractual;

b) Las llamadas de quienes hayan sido expresamente permitidos por el titular o usuario autorizado de los servicios de telefonía en cualquiera de sus modalidades, inscripto en el Registro Nacional "No Llame".

Artículo 53 ° .- Condiciones de contacto. Los contactos telefónicos de publicidad, oferta, venta y regalo de bienes o servicios no solicitados deben realizarse desde un número visible por el identificador de llamadas u otra tecnología que posea el titular o usuario de la línea telefónica.
En todos los casos, los contactos telefónicos, incluso a personas no inscriptas en el Registro Nacional "No Llame" o bajo el amparo de alguna de las excepciones previstas en el artículo 52, deben ser realizadas en forma y horario razonables y de acuerdo a lo que establezca la reglamentación.

Artículo 54 ° .- Denuncias. El titular o usuario autorizado del servicio de telefonía en cualquiera de sus modalidades puede realizar la denuncia por incumplimiento del presente Capítulo ante la autoridad de control dentro del plazo de UN (1) mes contado desde el momento del contacto.

Artículo 55 ° .- Incumplimientos. La autoridad de control iniciará actuaciones administrativas en caso de presuntas infracciones a las disposiciones del presente Capítulo, aplicando el procedimiento previsto en el artículo 65, párrafos tercero y cuarto. Verificada la existencia de la infracción, quienes la hayan cometido serán pasibles de las sanciones previstas en el artículo 69.

Artículo 56 ° .- Recepción de prueba. La autoridad de control, a los fines probatorios, tendrá en cuenta los elementos de hecho e indicios de carácter objetivos aportados por el denunciante que sustenten la situación fáctica debatida, quedando a cargo del denunciado acreditar que ha dado cumplimiento con las obligaciones establecidas en el presente Capítulo.
A requerimiento de la autoridad de control, los sujetos obligados deberán brindar el registro de sus llamadas salientes provisto por la empresa prestadora del servicio de telecomunicaciones de la que fueran usuarios, quien lo debe proveer en un plazo máximo de DIEZ (10) días y en las condiciones que la autoridad de control disponga.
En el marco de un sumario administrativo por incumplimientos al presente Capítulo, la autoridad de control podrá requerir en un plazo razonable informes a las empresas prestadoras del servicio de telecomunicaciones sobre:
a) La existencia del contacto telefónico cuestionado;
b) La información de la titularidad de una línea telefónica.
El incumplimiento de la requisitoria a que se refieren los párrafos segundo y tercero hará pasibles a las empresas prestadoras del servicio de telecomunicaciones de las sanciones previstas en el artículo 69, inciso b).

Artículo 57°. Resolución. La autoridad de control dictará la resolución que corresponda dentro de los TREINTA (30) días de recibida la prueba y producidos los alegatos si corresponden. La autoridad de control podrá prorrogar este plazo cuando la complejidad del tema a resolver sea fundamento suficiente para esa prórroga.
La resolución de la autoridad de control podrá:
a) Archivar la denuncia;

b) Imponer una sanción en caso de que se hubiera verificado un incumplimiento al presente Capítulo.

La resolución de la autoridad de control mencionada en el inciso b) agotará la vía administrativa a los efectos de lo previsto en la Ley Nacional de Procedimientos Administrativos Nº 19.549 y sus modificatorias. No procederá el recurso de alzada. Agotada la vía administrativa, la resolución será recurrible por ante la CÁMARA NACIONAL DE APELACIONES EN LO CONTENCIOSO ADMINISTRATIVO FEDERAL de la CAPITAL FEDERAL.

CAPÍTULO 6
SUPUESTOS ESPECIALES

Artículo 58 ° .- Bases de datos públicas. La creación, modificación o supresión de bases de datos pertenecientes a autoridades u organismos públicos debe hacerse por medio de norma de alcance general, publicada en el Boletín Oficial o diario oficial.

Las normas respectivas, deben indicar:

a) Órganos responsables de la base de datos, precisando dependencia jerárquica en su caso;

b) Características y finalidad de los tratamientos de datos que se efectúen;

c) Personas respecto de las cuales se pretenda obtener datos y el carácter facultativo u obligatorio de su suministro por parte de aquéllas;

d) Procedimiento de obtención y actualización de los datos;

e) Estructura básica de la base y la descripción de la naturaleza de los datos personales que contendrán;

f) Las cesiones, transferencias o interconexiones previstas;

g) Las oficinas ante las que se pudiesen efectuar el ejercicio de los derechos previstos en la presente Ley.

En las normas que se dicten para la supresión de las bases de datos se debe establecer el destino de éstas o las medidas que se adopten para su destrucción.

Artículo 59 ° .- Tratamiento de datos por organismos de seguridad e inteligencia. Las bases de datos de las Fuerzas Armadas, Fuerzas de Seguridad, organismos policiales o de inteligencia quedan sujetos a las disposiciones de la presente Ley. Las Comisiones Bicamerales de FISCALIZACIÓN DE ORGANISMOS Y ACTIVIDADES DE INTELIGENCIA y de FISCALIZACIÓN DE ÓRGANOS Y ACTIVIDADES DE SEGURIDAD INTERIOR del HONORABLE CONGRESO DE LA NACIÓN y la COMISIÓN DE DEFENSA NACIONAL de la HONORABLE CÁMARA DE SENADORES DE LA NACIÓN, o las que las sustituyan, tienen acceso a las bases de datos mencionadas por razones fundadas y en aquellos aspectos que constituyan materia de competencia de tales comisiones.

El tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las Fuerzas Armadas, Fuerzas de Seguridad, organismos policiales o de inteligencia, cuando sea necesario realizar sin el consentimiento del titular, queda limitado a aquellos supuestos y categorías de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquéllos para la defensa nacional, la seguridad pública o para la represión de los delitos.

Se deben suprimir, aun si no medie solicitud del titular, los datos personales de las bases de datos mencionadas en el primer párrafo cuando no sean necesarios para los fines que motivaron su recolección.

Artículo 60 ° .- Prestación de servicios de información crediticia del sector financiero y no financiero. En la prestación de servicios de información crediticia sólo pueden tratarse datos personales de carácter patrimonial relativos a la solvencia económica y al crédito, obtenidos de fuentes de acceso público irrestricto o restricto, o procedentes de informaciones facilitadas por el titular de los datos o con su consentimiento.

Pueden tratarse igualmente datos personales relativos al cumplimiento o incumplimiento de obligaciones de contenido patrimonial, facilitados por el acreedor o por quien actúe por su cuenta o interés.

A solicitud del titular de los datos, el responsable o encargado del tratamiento debe comunicar a aquél en forma gratuita las informaciones, evaluaciones y apreciaciones que sobre él hayan sido comunicadas durante los últimos DOCE (12) meses y la fuente de la información, incluyendo nombre y domicilio, en caso de corresponder.

Sólo se pueden archivar, registrar o ceder los datos personales que sean significativos para evaluar la solvencia económico financiera de los afectados durante los últimos CINCO (5) años a contar desde la última información significativa, o desde el vencimiento del plazo original de la operación de crédito de que se trate, el que fuera mayor. El plazo se reduce a DOS (2) años cuando el deudor cancele o extinga la obligación, a contar a partir de la fecha precisa en que se extingue la deuda. Se considera información significativa:

a) El momento en que se produce la mora del deudor;

b) Las distintas calificaciones que le otorgan al deudor las entidades crediticias;

c) El inicio de la acción judicial de cobro;

d) La sentencia judicial que dispone el pago de la deuda;

e) La fecha de la apertura del concurso de acreedores o de la declaración de quiebra, en caso de deudas verificadas o en trámite de verificación en los procesos de concursos preventivos y quiebras respectivamente;

f) Aquella otra información que defina el órgano de control.

No se considera última información significativa la asentada en una base de datos por el sólo hecho de ser la constancia final de una serie o sucesión de datos si se trata de una mera repetición de la misma información que, sin novedad o aditamento alguno, ha sido archivada durante los meses anteriores.

De conformidad con lo establecido en el artículo 14 de la presente, no es necesario el consentimiento en los siguientes casos:

a) Cuando se trate de las operaciones que realicen las entidades crediticias y de las informaciones que reciban de sus clientes, conforme las disposiciones del artículo 39 de la Ley de Entidades Financieras Nº 21.526 y sus modificaciones.

b) Prestación de servicios de información crediticia por parte de entidades crediticias y empresas que presten el servicio de dicha información, a los efectos de su cesión, ni la ulterior comunicación de ésta, o de su transferencia internacional, cuando estén relacionados con el giro de las actividades comerciales o crediticias de los cesionarios.

Las entidades crediticias deberán ceder, en las condiciones que se indican a continuación, la información relativa al cumplimiento de obligaciones de contenido patrimonial exclusivamente al BANCO CENTRAL DE LA REPÚBLICA ARGENTINA y, desde el mismo se pondrá dicha información a disposición de los responsables o encargados del tratamiento que prestan servicios de información crediticia, acreedores y otros interesados. Esta obligación no afectará bajo ninguna medida el derecho de acceso de los titulares de los datos.

Las entidades crediticias que obligatoriamente cedan información relativa al cumplimiento de obligaciones de contenido patrimonial al BANCO CENTRAL DE LA REPÚBLICA ARGENTINA, deben comunicar al titular de los datos la información a ceder al último domicilio por él denunciado o por un canal de comunicación habitual entre las partes que permita acreditar el envío y su fecha. A tales fines, dicha comunicación puede remitirse por medio postal o electrónico y junto con otras comunicaciones, como ser la de sus consumos, movimientos de cuenta, recibos o facturas. En cualquier caso, el cedente tiene la carga de acreditar el cumplimiento de la comunicación aquí dispuesta. Esta comunicación se debe efectuar cuando las obligaciones pasen de cumplimiento normal a incumplimiento, sin que se deba comunicar al deudor la continuidad de tal incumplimiento y/o el agravamiento de la calificación, y dentro de los DIEZ (10) días hábiles de producida la nueva calificación.

En caso de disconformidad con el contenido de la información comunicada conforme al párrafo precedente, el titular de los datos puede ejercer los derechos que le correspondan de acuerdo a lo establecido en esta Ley.

Respecto de la información crediticia del sector no financiero, previo a ceder datos personales relativos al incumplimiento de obligaciones patrimoniales a responsables o encargados del tratamiento que prestan servicios de

información crediticia, los cedentes deben comunicar al titular de los datos la información a ceder y sus cesionarios al último domicilio por él denunciado o por un canal de comunicación habitual entre las partes que permita acreditar el envío y su fecha. A tales fines, dicha comunicación puede remitirse por medio postal o electrónico y junto con otras comunicaciones, como ser la de sus consumos, movimientos de cuenta, recibos o facturas. En cualquier caso, el cedente tiene la carga de acreditar el cumplimiento de la comunicación aquí dispuesta. Una vez cursada dicha comunicación al titular de los datos, no se requiere una nueva para realizar otras cesiones referidas a la misma obligación, en tanto se le haya informado al titular de los datos en la comunicación respectiva todos los cesionarios a los que se cedieran o previesen ceder sus datos personales. Los tratamientos de datos efectuados por el Estado quedan exceptuados de la notificación dispuesta en el presente párrafo.

En caso de disconformidad con el contenido de la información a ceder conforme al párrafo precedente, el titular de los datos puede ejercer cualquiera de los derechos que le correspondan de acuerdo a lo establecido en esta Ley.

La información puede ser difundida por el sector no financiero luego de transcurridos DIEZ (10) días hábiles de enviada la comunicación. Si el titular de los datos cumple con su obligación dentro de dicho plazo, no podrán cederse tales datos a las empresas que prestan servicios de información crediticia.

Cuando se deniegue al titular de los datos la celebración de un contrato, solicitud de trabajo, servicio, crédito comercial o financiero, sustentado en un informe crediticio, deberá informársele tal circunstancia, así como la empresa que proveyó dicho informe y hacerle entrega de una copia de éste.

Se debe suprimir la información relativa a los fiadores o avalistas cuando se haya cancelado o extinguido la obligación, previo pedido por parte del deudor, fiador o avalista ante la empresa de información crediticia, en la modalidad y plazos dispuestos por el artículo 34 de la presente Ley.

En el caso de los archivos o bases de datos públicas conformadas por cesión de información suministrada por entidades crediticias, de conformidad con el párrafo 8 del artículo 60 de la presente, los derechos de rectificación, oposición

y supresión deben ejercerse ante la entidad cedente que sea parte en la relación jurídica a que se refiere el dato impugnado. De no conocer cuál habría sido la entidad cedente de la información, el titular de los datos tiene derecho a consultar a la entidad cesionaria los datos de la entidad cedente. Si procediera el reclamo, la entidad respectiva debe solicitar al BANCO CENTRAL DE LA REPÚBLICA ARGENTINA, o a la Autoridad de Aplicación, según el caso, que sean practicadas las modificaciones necesarias en sus bases de datos. Toda modificación debe ser comunicada a través de los mismos medios empleados para la divulgación de la información.

Artículo 61 ° .- Bases destinadas a la publicidad. Pueden tratarse sin consentimiento de su titular datos personales con fines de publicidad, venta directa y otras actividades análogas, cuando estén destinados a la formación de perfiles determinados o que permitan establecer hábitos de consumo que categoricen preferencias y comportamientos similares de las personas, siempre que los titulares de los datos sólo se identifiquen por su pertenencia a tales grupos genéricos, con más los datos individuales estrictamente necesarios para formular la oferta a los destinatarios.

En toda comunicación con fines de publicidad que se realice por correo, teléfono, correo electrónico, Internet u otro medio que permita la tecnología en el futuro, el responsable o encargado del tratamiento debe implementar medidas razonables que informen al titular de los datos la posibilidad de ejercer los derechos previstos en la presente Ley.

Los datos referentes a la salud sólo pueden ser tratados, a fin de realizar ofertas de bienes y servicios, cuando hubieran sido obtenidos de acuerdo con la presente Ley y siempre que no causen discriminación, en el contexto de una relación entre el consumidor o usuario y los proveedores de servicios o tratamientos médicos y entidades sin fines de lucro. Estos datos no pueden cederse a terceros sin el consentimiento previo, expreso e informado del titular de los datos. A dicho fin, este último debe recibir una noticia clara del carácter sensible de los datos que proporciona y de que no está obligado a

suministrarlos, junto con la información del artículo 15 y la mención de su derecho a oponerse al tratamiento de sus datos.

En los supuestos contemplados en el presente artículo, el titular de los datos puede ejercer el derecho de acceso sin cargo ni limitación temporal alguna. La información a suministrársele debe incluir la fuente de la que se obtuvieron sus datos, indicando, en su caso, el nombre del responsable o encargado del tratamiento que proveyó la información.

CAPÍTULO 7
AUTORIDAD DE CONTROL

Artículo 62 ° .- Autoridad de control. La AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA, creada por la Ley No 27.275, será la autoridad de control que debe velar por el cumplimiento de los principios y procedimientos establecidos en la presente Ley.

Artículo 63 ° .- Facultades de la autoridad de control. La autoridad de control tendrá las siguientes funciones y atribuciones:

a) Asistir y asesorar a las personas que lo requieran acerca de los alcances de la presente Ley y de los medios legales de que disponen para la defensa de sus derechos;

b) Dictar las normas y criterios orientadores que se deben observar en el desarrollo de las actividades comprendidas por esta Ley; específicamente, dictar normas administrativas y de procedimiento relativas a las funciones a su cargo, y las normas y procedimientos técnicos relativos al tratamiento de datos y condiciones de seguridad de las bases de datos;

c) Atender los requerimientos y denuncias interpuestos en relación al tratamiento de datos en los términos de la presente Ley;

d) Controlar el cumplimiento de los requisitos y garantías que deben reunir los tratamientos de datos de conformidad con la presente Ley y las normas que dicte la autoridad de control; a tal efecto, podrá solicitar autorización judicial

para acceder a locales, equipos, o programas de tratamiento de datos a fin de verificar infracciones al cumplimiento de esta Ley. La autorización judicial deberá especificar el alcance y modalidad de la inspección, asegurando que se adopten medidas apropiadas para proteger la confidencialidad de datos personales de terceros no involucrados en la investigación, la propiedad intelectual del inspeccionado, y minimizar la interrupción de las operaciones. Cuando el tratamiento se realice en infraestructura compartida o mediante servicios tecnológicos que procesen datos de múltiples clientes, la autoridad de control deberá considerar métodos de auditoría alternativos, incluyendo certificación de revisiones emitidas por organismos independientes reconocidos internacionalmente, informes de auditoría de terceros o inspecciones remotas, cuando sean suficientes para verificar el cumplimiento;

e) Solicitar información a las entidades públicas y privadas, las que deberán proporcionar los antecedentes, documentos, programas u otros elementos relativos al tratamiento de datos que se le requieran; en estos casos, la autoridad deberá garantizar la seguridad y confidencialidad de la información y elementos suministrados;

f) Imponer las sanciones administrativas que, en su caso, correspondan por violación a las normas de la presente Ley y de las reglamentaciones que se dicten en su consecuencia;

g) Percibir las tasas que se fijen por Ley por los servicios de inscripción y otros que preste;

h) Constituirse en querellante en las acciones penales que se promovieran por violaciones a la presente Ley;

i) Homologar los mecanismos de autorregulación vinculantes y supervisar su cumplimiento;

j) Solicitar información a los delegados de protección de datos, en los términos de lo previsto en la presente Ley;

k) Elaborar y presentar ante el HONORABLE CONGRESO DE LA NACIÓN propuestas de reforma legislativa respecto de su área de competencia;

l) 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.

CAPÍTULO 8
PROCEDIMIENTOS Y SANCIONES

Artículo 64°- Procedimiento. A los efectos de constatar el cumplimiento de las disposiciones de la presente Ley, la autoridad de control podrá iniciar procedimientos:

a) A instancias del titular de los datos o de su representante legal;

b) De verificación de oficio;

c) De verificación por denuncia de un tercero.

La autoridad de control podrá en cualquier momento del procedimiento buscar una conciliación entre el titular de los datos y el responsable del tratamiento. De llegarse a un acuerdo de conciliación entre ambos, esté se hará constar por escrito y tendrá efectos vinculantes.

La autoridad de control determinará el procedimiento que se aplicará a la conciliación.

Artículo 65 ° .- Trámite de protección de los datos personales. El titular de los datos o su representante legal puede iniciar un trámite de protección de los datos personales presentando ante la autoridad de control una solicitud, de manera escrita y por cualquier medio habilitado por la autoridad de control, expresando con claridad el contenido de su requerimiento y de los preceptos de esta Ley que se consideran vulnerados. La presentación debe realizarse ante la autoridad de control dentro de los TREINTA (30) días siguientes a la fecha en que se comunique la respuesta al titular de los datos por parte del responsable del tratamiento, de acuerdo a lo previsto en el artículo 34, párrafos segundo y tercero, de la presente Ley.

En el caso de que el titular de los datos no reciba respuesta por parte del responsable del tratamiento dentro de los DIEZ (10) días hábiles de haber intimado fehacientemente, basta que el titular de los datos acredite la fecha en que presentó la solicitud ante el responsable del tratamiento.
Iniciado el trámite de protección de los datos personales previsto en este artículo ante la autoridad de control, se dará traslado de aquél al responsable del tratamiento, para que en el plazo de DIEZ (10) días hábiles, emita respuesta, ofrezca las pruebas que estime pertinentes y manifieste por escrito lo que a su derecho convenga.
La autoridad de control admitirá las pruebas que estime pertinentes. Asimismo, podrá solicitar del responsable del tratamiento las demás pruebas que considere necesarias. Concluida la recepción de pruebas, la autoridad de control notificará al responsable del tratamiento el derecho que le asiste para que, de considerarlo necesario, presente sus alegatos dentro de los CINCO (5) días hábiles siguientes a su notificación.

Artículo 66 ° .- Trámite de verificación de oficio o por denuncia de un tercero.
La autoridad de control verificará el cumplimiento de la presente Ley y de la normativa que de ésta derive. La verificación podrá iniciarse de oficio o por denuncia de un tercero.
A efectos de practicar la verificación, la autoridad de control tendrá acceso a la información y documentación que considere necesarias, de acuerdo a lo previsto en la presente Ley y a la reglamentación correspondiente.
En caso de que corresponda, se aplicará al trámite lo previsto en el artículo 65, párrafos tercero y cuarto, de la presente Ley.

Artículo 67 ° .- Resolución. La resolución de la autoridad de control podrá:
a) Archivar los trámites mencionados en los artículos 65 y 66 de la presente Ley;

b) En caso de considerar que asiste derecho al titular de los datos, requerirle al responsable del tratamiento que haga efectivo el ejercicio de los derechos

objeto de protección, debiendo dar cuenta por escrito de dicho cumplimiento a la autoridad de control dentro de los QUINCE (15) días hábiles de efectuado;

c) De verificarse incumplimientos a la presente Ley, imponer una sanción de las previstas en el artículo 69.

d) La autoridad de control dictará la resolución que corresponda dentro de un plazo razonable, atendiendo a la complejidad del tema a resolver.

Artículo 68 ° .- Recursos. Las resoluciones de la autoridad de control agotarán la vía administrativa a los efectos de lo previsto en la Ley Nacional de Procedimientos Administrativos Nº 19.549 y sus modificatorias. No procederá el recurso de alzada. Agotada la vía administrativa, las resoluciones previstas en el artículo 69 serán recurribles por ante la CÁMARA NACIONAL DE APELACIONES EN LO CONTENCIOSO ADMINISTRATIVO FEDERAL de la CAPITAL FEDERAL.

Artículo 69 ° .- Sanciones. Una vez establecido el incumplimiento de las disposiciones de la presente Ley por parte del responsable del tratamiento o del encargado del tratamiento, la autoridad de control impondrá las medidas o las sanciones correspondientes.
La autoridad de control podrá imponer a los responsables y encargados del tratamiento las siguientes sanciones:
a) Apercibimiento;

b) Multa que podrá alcanzar CINCO MIL NOVECIENTOS VEINTICINCO (5.925) Salarios Mínimos Vitales y Móviles vigentes al momento de la imposición de la sanción como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % (DOS POR CIENTO) como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía;

c) Suspensión de las actividades relacionadas con el tratamiento de datos hasta por un término de SEIS (6) meses; en el acto de suspensión se indicarán los correctivos que se deberán adoptar;

d) Cierre temporal de las operaciones relacionadas con el tratamiento de datos una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la autoridad de control;

e) Cierre inmediato y definitivo de la operación que involucre el tratamiento de datos sensibles.

Al ordenar la suspensión o cierres previstos en los incisos c), d) y e) la autoridad de control podrá ordenar que, de manera temporal o definitiva, se retire, bloquee, suspenda y/o inhabilite el acceso a los datos personales a los que los responsables del tratamiento den acceso, interconecten, transmitan o direccionen, almacenen, alojen, intermedien, enlacen o busquen, que lesionen derechos legalmente reconocidos. A tal efecto, la autoridad de control deberá precisar, de acuerdo a lo informado por el titular de los datos, el enlace en el que se encuentren alojados los datos personales o los procedimientos para acceder a aquél.

En ningún caso, estas medidas podrán afectar el derecho a la libertad de expresión e información.

Las sanciones indicadas en el presente artículo sólo se aplican para las personas de naturaleza privada. En el caso en el cual la autoridad de control advierta un presunto incumplimiento de una autoridad pública a las disposiciones de la presente Ley, remitirá la actuación a la autoridad que corresponda para que inicie la investigación respectiva.

En todos los casos, la autoridad de control podrá disponer, a costa del responsable, la publicación de la resolución en el diario de mayor circulación de la jurisdicción donde se encuentre establecido el responsable.

Artículo 70°. Gradación. Las sanciones por infracciones a las que se refiere el artículo 69 se graduarán atendiendo los siguientes criterios, en cuanto resulten aplicables:

a) La 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 control;

e) El incumplimiento de los requerimientos u órdenes impartidas por la autoridad de control;

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

La designación voluntaria de un Delegado de Protección de Datos, la adopción de mecanismos de autorregulación vinculantes, la realización de una evaluación de impacto en los términos del artículo 40 y la notificación oportuna de incidentes de seguridad, serán merituados como atenuantes de la sanción que corresponda, sin perjuicio de otros que pueda considerar la autoridad de control.

CAPÍTULO 9
ACCIÓN DE HABEAS DATA

Artículo 71 ° .- Procedencia. La acción de hábeas data procede para tutelar los derechos que resulten restringidos, alterados, lesionados o amenazados por un tratamiento de datos personales contrario a la presente Ley por parte de las autoridades públicas o por particulares. Esta acción procederá especialmente para ejercer los derechos de acceso, rectificación, oposición, cancelación y portabilidad de los datos previstos en la presente Ley.

En los casos en que se presuma o se hubiera verificado la falsedad, inexactitud, desactualización de la información de que se trata, o se hubiera realizado un tratamiento de datos ilícito o prohibido, la acción de hábeas data procederá para ejercer los derechos de rectificación, de oposición, o de

supresión previstos en los artículos 29, 30 y 31; el derecho de oposición también podrá ser ejercido en los supuestos del artículo 32 de la presente Ley.

Artículo 72°.- Legitimación activa y pasiva. La acción de habeas data podrá ser ejercida por el titular de los datos afectados, sus tutores, curadores o por el titular de la responsabilidad parental o tutela en caso de niños, niñas o adolescentes. En el caso de las personas humanas fallecidas, la acción podrá ser ejercida por sus sucesores universales.
La acción podrá ser también intentada en representación plural, sectorial o colectiva, siempre que su objeto se limite a la impugnación de tratamientos que conllevan violaciones generalizadas, pero en tal caso los promotores de tales acciones no podrán tener acceso a los datos de las demás personas que integran el colectivo por ellas representados, sino sólo a los datos propios.
Tendrán legitimación para interponer esta acción el titular de los datos, el DEFENSOR DEL PUEBLO, las asociaciones sectoriales, la autoridad de control y el MINISTERIO PÚBLICO.
En el proceso podrá intervenir, en forma coadyuvante y cuando corresponda, la autoridad de control, quien será notificada del inicio de la acción de habeas data.
La acción procede respecto de los responsables del tratamiento.
Excepcionalmente los responsables del tratamiento podrán interponer la acción contra otros responsables o encargados del tratamiento cuando éstos últimos incumplan con sus obligaciones legales o convencionales y esto pueda acarrearles perjuicio.

Artículo 73 ° .- Competencia. Será competente para entender en esta acción el juez del domicilio del actor o del demandado, a elección del actor.
Procederá la competencia federal cuando la acción:
a) Se interponga en contra de los responsables del tratamiento que sean parte de la Administración Pública Nacional;

b) Se interponga en contra del responsable del tratamiento de datos accesibles en redes interjurisdiccionales, nacionales o internacionales.

Artículo 74 ° .- Procedimiento aplicable. La acción de hábeas data tramitará según las disposiciones de la presente Ley y, supletoriamente, según el procedimiento que corresponde a la acción de amparo común y según las normas del CÓDIGO PROCESAL CIVIL Y COMERCIAL DE LA NACIÓN, en lo atinente al juicio sumarísimo.
El juez dispondrá de amplias facultades para adaptar los procedimientos de acuerdo a las circunstancias particulares del caso y a fin de dar mayor eficacia tuitiva al proceso.

Artículo 75 ° .- Requisitos de la demanda. La demanda deberá interponerse por escrito, individualizando con la mayor precisión posible el nombre y domicilio del responsable del 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 procurará establecer autoridad u organismo público del cual dependan el responsable o el encargado del 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. Deberá asimismo, 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 del tratamiento informe que la información cuestionada está sometida 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 76 ° .- Trámite. Admitida la acción, el juez requerirá al responsable del tratamiento la remisión de la información concerniente al accionante y el ofrecimiento de la prueba pertinente. Podrá asimismo solicitar, en caso que corresponda, esa información al encargado del tratamiento o al delegado de protección de datos. También podrá requerir informes sobre el soporte técnico de datos, documentación de base relativa a la recolección y cualquier otro aspecto que resulte conducente a la resolución de la causa que estime procedente.

El plazo para contestar el informe no podrá ser mayor de CINCO (5) días hábiles, el que podrá ser ampliado prudencialmente por el juez.

Los responsables o encargados del tratamiento o Delegados de Protección de Datos no podrán alegar la confidencialidad de la información que se les requiere, salvo el caso en que se afecten las fuentes de información periodística.

Cuando un responsable o encargado del tratamiento o Delegado de Protección de Datos se oponga a la remisión del informe solicitado, con invocación de las excepciones autorizadas por la presente Ley o por una Ley específica, deberá 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 77 ° .- Contestación del informe. Al contestar el informe, el responsable o encargado del tratamiento o el Delegado de Protección de Datos deberá expresar las razones por las cuales efectuó el tratamiento cuestionado y, en su caso, aquellas razones por las que no evacuó el pedido efectuado por el accionante.

Artículo 78 ° .- Ampliación de la demanda. Contestado el informe, el actor podrá, en el término de TRES (3) días, ampliar el objeto de la demanda, ofreciendo en el mismo acto la prueba pertinente. De esta presentación se dará traslado al demandado por igual término para que conteste y ofrezca prueba.

Artículo 79 ° .- Sentencia. Vencido el plazo para la contestación del informe o contestado éste, y en el supuesto del artículo 78, luego de contestada la ampliación y en su caso, habiendo sido producida la prueba, el juez dictará sentencia.

En el caso de estimarse procedente la acción, se especificará si la información debe ser bloqueada, suprimida, rectificada, o actualizada, estableciendo un plazo para su cumplimiento. En ningún caso, la sentencia podrá afectar el derecho a la libertad de expresión e información.

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

En cualquier caso, la sentencia deberá ser comunicada a la autoridad de control.

Contra la sentencia procede el recurso de apelación.

CAPÍTULO 10
DISPOSICIONES TRANSITORIAS

Artículo 80 ° .- Reglamentación. El PODER EJECUTIVO NACIONAL reglamentará la presente Ley dentro de los CIENTO OCHENTA (180) días desde su promulgación.

Artículo 81 ° .- Vigencia. Las disposiciones de la presente Ley entrarán en vigencia a los DOS (2) años de su publicación en el Boletín Oficial.

Los responsables y encargados del tratamiento contarán con el plazo máximo de DOS (2) años desde la publicación de la presente Ley en el Boletín Oficial, para adaptarse a las obligaciones contenidas en ella. En dicho plazo, conservarán plena vigencia las Leyes Nros. 25.326, 26.343 y 26.951, sus normas reglamentarias y las demás disposiciones que hubieran sido dictadas por la DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES y/o la AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA.

El Registro Nacional "No Llame", creado por la Ley Nº 26.951, será transferido al nuevo registro creado por el artículo 46 de la presente Ley de acuerdo a lo que prevea su reglamentación.

CAPÍTULO 11
DISPOSICIONES FINALES

Artículo 82 ° .- Orden público y jurisdicción federal. Las normas de la presente Ley contenidas en los Capítulos 1, 2, 3, 4, 6 y 11 son de orden público y de aplicación en lo pertinente en todo el territorio nacional.
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.
La competencia federal regirá respecto de:
a) Los tratamientos de datos efectuados por las autoridades u organismos públicos pertenecientes a la Administración Pública Nacional;

b) Los tratamientos de datos efectuados por el sector privado, cuando los datos se encuentren accesibles en redes interjurisdiccionales, nacionales o internacionales.

Artículo 83 ° .- Referencias. Toda referencia normativa a la DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES que dependía del MINISTERIO DE JUSTICIA como autoridad de control de la Ley de Protección de Datos Personales, a su competencia o sus autoridades, se considerará referida a la AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA.

Artículo 84 ° .- Derogación. Deróganse las Leyes Nros 25.326, 26.343 y 26.951.

Artículo 85 ° .- Comuníquese al PODER EJECUTIVO NACIONAL.

Autora:
BANFI, Karina

FUNDAMENTOS

Señor presidente:

El presente proyecto tiene por finalidad establecer un nuevo ordenamiento legal sobre la protección de los datos personales y encuentra antecedentes en los proyectos presentados bajo los expedientes 6234-D-2020, 4081-D-2022 y 0311-D-2024, con algunas mínimas actualizaciones.

Para su elaboración se tomó como base el texto "Nueva versión del anteproyecto de Ley de Protección de Datos Personales", que se encuentra publicado en el sitio web oficial de la Agencia de Acceso a la Información Pública, así como algunos elementos del Proyecto de Ley de Protección de Datos Personales que el Poder Ejecutivo Nacional envió al Honorable Congreso de la Nación en septiembre de 2018, por Mensaje MEN-2018-147-APN-PTE.

Aunque la presente iniciativa integra elementos de ambos textos e introduce cambios respecto de ellos, vale explicar las razones por las que esas versiones han sido utilizadas como punto de partida para la elaboración del presente Proyecto.

En primer lugar, en junio de 2019 durante la visita oficial a Argentina de Vera Jourová -por entonces Comisaria Europea de Justicia, Consumidores e Igualdad de Género de la Comisión Europea- me comprometí a impulsar la modernización de la legislación argentina en materia de protección de datos personales, y en particular, el Proyecto de Ley de Protección de Datos Personales que fuera presentado por el Poder Ejecutivo en 2018 (MEN-2018-147-APN-PTE).

En segundo lugar, el anteproyecto publicado por la Agencia de Acceso a la Información Pública es valioso no solo porque fue elaborado inicialmente por el organismo que posee el expertise técnico en la materia, sino porque también incorpora aportes y comentarios que esa Agencia recibió desde distintos sectores -organismos públicos, empresas, academia, sociedad civil- durante su elaboración.

Como surge del sitio web de la Agencia de Acceso a la Información Pública, la elaboración del texto "Nueva versión del anteproyecto de Ley de Protección de Datos Personales" -y que se tomó como base para la presente iniciativa- se realizó en el marco del programa "Justicia 2020", creado por el Ministerio de Justicia y Derechos Humanos. Dicho programa funcionó como un espacio de participación ciudadana e institucional para la elaboración, implementación y seguimiento de iniciativas y políticas de Estado, y tuvo dos etapas.

Durante la primera, se realizaron reuniones de trabajo para debatir los principales ejes y desafíos que presenta en la actualidad la protección de los datos personales. Las reuniones se realizaron entre los meses de agosto y noviembre de 2016. En este proceso de deliberación participaron actores interesados en la materia, provenientes del sector privado, del ámbito académico y de la sociedad civil, tanto locales como extranjeros. El resultado de esas reuniones fue compilado y publicado en el documento "Ley de Protección de los Datos Personales en Argentina (Sugerencias y aportes recibidos en el proceso de reflexión sobre la necesidad de su reforma - Agosto-Diciembre 2016)". Ese documento fue elaborado por la ex Dirección Nacional de Protección de Datos Personales de la Subsecretaría de Asuntos Registrales del Ministerio de Justicia y Derechos Humanos.

Asimismo, dicha Dirección Nacional de Protección de Datos Personales prestó la colaboración técnica para la elaboración de un anteproyecto en el que se tuvieron en cuenta regulaciones existentes a nivel internacional específicas en la materia, como el Reglamento (UE) 2016/679, el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento

automatizado de datos de carácter personal (Convenio 108) y el Convenio sobre la Ciberdelincuencia (Convención de Budapest) y legislación comparada que ha sido sancionada en los últimos años: la Ley Federal de Protección de Datos Personales en Posesión de los Particulares de los Estados Unidos Mexicanos y su respectiva reglamentación, la Ley de Protección de Datos Personales Nº 29.733 de la República de Perú y su respectiva reglamentación, la Ley Estatutaria 1581 de 2012 de la República de Colombia y su respectiva reglamentación, y la Ley de Protección de Información Personal y de Documentos Electrónicos de Canadá (Personal Information Protection and Electronic Documents Act - PIPEDA), entre otras. También se tuvieron en cuenta los Estándares de Protección de Datos Personales para los Estados Iberoamericanos (Red Iberoamericana de Protección de Datos - Documento en elaboración) y el Informe del Comité Jurídico Interamericano sobre Privacidad y Protección de Datos Personales.

La segunda etapa del proceso realizado en el marco del Programa Justicia 2020 se realizó durante los primeros meses del año 2017. En esa oportunidad el anteproyecto mencionado fue puesto a discusión pública, recibiéndose comentarios y sugerencias de similares sectores que habían participado en la primera fase del proceso.

Habiendo explicado lo anterior, cabe referirse a continuación a las razones concretas que motivan la presente iniciativa.

La protección de los datos personales se encuentra regulada en nuestro país a través de la acción de habeas data, incorporada en oportunidad de la Reforma Constitucional del año 1994 en el artículo 43, tercer párrafo, de la Constitución Nacional. Posteriormente, en el año 2000 se sancionó la Ley N° 25.326, norma de orden público que regula los principios aplicables en la materia y el procedimiento de la acción de habeas data. Por último, en diciembre de 2018 mediante la Ley Nº 27.483 se aprobó el Convenio del Consejo de Europa para la Protección de las Personas con respecto al tratamiento automatizado de datos de carácter personal, usualmente denominado “Convenio 108”, en

vigencia respecto de la República Argentina desde junio de 2019. Además de regular principios y garantías básicas en la materia, el Convenio 108 contiene obligaciones respecto de la independencia de la autoridad de control en los Estados Parte, así como obligaciones relativas al flujo transfronterizo de datos personales.

El objetivo del régimen propuesto es el de dotar a nuestro país de un régimen legal más moderno que respete los derechos y garantías establecidos por nuestra Constitución Nacional y que, al mismo tiempo, se adapte a las nuevas tecnologías y a los cambios regulatorios ocurridos en el derecho comparado durante los últimos años.

Es innegable que la evolución de la tecnología en los últimos veinte años, además de haber producido beneficios innegables para el ejercicio de múltiples derechos, ha impactado en la protección de los datos personales con el surgimiento de nuevas vulneraciones al derecho a la privacidad. Asimismo, se debe recalcar el nuevo contexto internacional en la materia, particularmente las nuevas regulaciones en Europa que han sido recientemente aprobadas; tal es el caso del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante "Reglamento (UE) 2016/679"), que ha entrado en vigencia en mayo de 2018. Cabe destacar que la República Argentina desde el año 2003 es considerada por la Unión Europea como un país con legislación adecuada para la protección de los datos personales (Comisión de las Comunidades Europeas - Decisión de la Comisión C (2003)1731 de fecha 30 de junio de 2003 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina). Sin perjuicio de esto, se advierte que, el estatus de país adecuado está siendo actualmente evaluado por la Comisión Europea a la luz de la entrada en vigencia del Reglamento (UE) 2016/679, motivo por el cual se propone la presente reforma con la finalidad de mantener los estándares internacionales a los que nuestra legislación supo adaptarse, lo

cual traerá consigo nuevas posibilidades de innovación e inversión en nuestro país.

La propuesta que se envía propicia la derogación de la Ley de Protección de los Datos Personales Nº 25.326 - y su modificatoria Nº 26.343 - y de la Ley Nº 26.951 –de creación, en el ámbito de la Dirección Nacional de Protección de Datos Personales dependiente del Ministerio de Justicia y Derechos Humanos, hoy en la Agencia de Acceso a la Información Pública, organismo descentralizado en la órbita de la Jefatura de Gabinete de Ministros-, del Registro Nacional "No Llame".

La necesidad de derogación de la Ley Nº 25.326, que fue sancionada hace más de veinte años, obedece a que, tal como se expresó anteriormente, ha quedado desactualizada dado los avances tecnológicos y normativos producidos desde entonces.

En el caso de la Ley Nº 26.951 y su modificación, por la cual se creó en el año 2014 el Registro Nacional "No Llame", se advirtieron falencias regulatorias que perjudicaron su aplicación e impidieron cumplir acabadamente con las expectativas de la población respecto de sus objetivos: entre ellos, evitar los abusos del procedimiento de contacto telefónico por parte de quienes ofrecen publicidad o venta de bienes y servicios. De allí la necesidad de sustituir la actual regulación legal por un nuevo régimen.

Entre las disposiciones generales contenidas en el Capítulo 1 del Proyecto, se incluye, en su artículo 2°, una serie de definiciones de conceptos que no figuran explícitamente en la Ley vigente. Así, por ejemplo, se han previsto definiciones de “datos biométricos” y “datos genéticos”, entre otros. A su vez, se redefinen ciertos términos cuya redacción en la Ley vigente es poco clara o restrictiva, como “datos personales” o “datos sensibles”. Asimismo, el concepto de “base de datos” se adecúa a los avances tecnológicos y siguiendo este mismo propósito, se incluyen definiciones sobre "disociación de datos" e “incidente de seguridad de datos personales”.

Una cuestión que es relevante destacar es que se ha optado por no incluir a las personas jurídicas como sujetos de los derechos fundamentales en virtud de que, según los estándares internacionales en la materia, las personas de existencia ideal no son sujetos titulares de derechos humanos fundamentales (Corte IDH, Opinión Consultiva OC - 22/16]). Ello es consistente también con lo dispuesto por el Protocolo que modifica el Convenio para la Protección de las Personas con respecto al tratamiento automatizado de datos de carácter personal -denominado usualmente como "Convenio 108+" o "Convenio 108 modernizado"-, que la República Argentina ha suscripto en el año 2019 y ratificado en el año 2022 mediante la aprobación de la ley 27699.

Asimismo, se aclara que el Proyecto tampoco prevé que se aplique la Ley en el supuesto de tratamiento de datos que efectúe una persona humana para su uso exclusivamente privado o de su grupo familiar (ver artículo 3º). El Proyecto modifica el criterio seguido por la Ley vigente y prescinde de utilizar conceptos jurídicos indeterminados, como "uso exclusivamente personal" o "destinados a dar informes", que han sido criticados no solo por la doctrina especializada sino también por la Unión Europea en la Decisión de la Comisión C (2003)1731, de fecha 30 de junio de 2003, que le dio a la República Argentina carácter de país adecuado. Por supuesto, se mantiene lo dispuesto en la normativa actual respecto de la exclusión de la aplicación de la ley en casos que se pueda afectar el secreto de las fuentes de información periodísticas (ver artículo 3º). Asimismo, y dada la relevancia que tienen los medios de comunicación y el ejercicio de la libertad de expresión en una sociedad democrática, tal como lo viene sosteniendo pacíficamente la Corte Interamericana de Derechos Humanos, expresamente se dispone que el tratamiento y la protección de los datos personales establecidos en esta Ley no se aplicará al tratamiento de datos que realicen los medios de comunicación en el ejercicio de la libertad de expresión.

Finalmente, respecto del ámbito de aplicación, el Proyecto sigue los lineamientos más modernos en la materia, entendiendo que la normativa se

aplicará en distintos supuestos, aun cuando los responsables de tratar los datos no se encuentren en territorio nacional (ver artículo 4º).

El Capítulo 2 contiene normas que permiten aclarar algunos de los principios aplicables relativos al tratamiento de datos, al mismo tiempo que incluye otros no previstos en la legislación actual, tales como el principio de minimización de los datos (ver artículo 7º) o el principio de responsabilidad proactiva (ver artículo 10). La inclusión de este último principio es uno de los cambios más importantes que trae la normativa proyectada, cuya necesidad de incorporación fue muy bien receptada durante todo el proceso que precedió a la elaboración del Proyecto. Al incorporar este principio, por el cual los responsables y otros sujetos que realizan tratamiento de datos se encuentran obligados a demostrar el cumplimiento de la ley, se abandona la obligación de registro de bases de datos, imposición que la experiencia ha demostrado poco útil y cuyo cumplimiento no ha sido del todo adecuado.

Otra cuestión que presenta el Proyecto, siguiendo iniciativas que provienen del derecho comparado, es la inclusión de previsiones específicas para aclarar el concepto del consentimiento del titular de los datos para su posterior tratamiento (ver artículos 12, 13 y 14). La regulación que propone el Proyecto es más acorde con el concepto correspondiente al estado de desarrollo conocido como "la era digital" y con las nuevas tecnologías. Ciertamente el consentimiento sigue siendo uno de los principios rectores para el tratamiento de datos personales, pero la propuesta incluye parámetros que admiten otorgarlo, de manera más clara, sin que ello impida la innovación y el avance de nuevas tecnologías y usos en internet.

El tratamiento de los datos sensibles (ver artículo 16) y el de los datos vinculados a antecedentes penales y contravencionales (ver artículo 17), se ha mantenido en el Proyecto con especificaciones que dan mayor claridad a los responsables o encargados del tratamiento. Otra novedad es que se decidió incorporar parámetros especiales para el tratamiento de datos de niñas, niños y adolescentes, resaltando la importancia que para ello tiene el respeto a la

Convención sobre los Derechos del Niño (ver artículo 18), la que fue aprobada por Ley Nº 23.849, y tiene jerarquía constitucional de conformidad con lo establecido por el artículo 75, inciso 22, segundo párrafo, de la Constitución Nacional.

En este mismo Capítulo, se incorporan también reglas aplicables a todos aquellos que hacen tratamiento de datos, especialmente la imposición legal de implementación de medidas de seguridad (ver artículo 19) y la obligación de notificar al titular de los datos y a la autoridad de control ante la ocurrencia de incidentes de seguridad (ver artículo 20). La exigencia de efectuar este tipo de notificación ante estos casos ha sido receptada por las legislaciones más modernas, con el fin de minimizar los perjuicios al titular de los datos, una vez ocurridos incidentes de seguridad.

Para finalizar, este Capítulo incluye especificaciones que aclaran o amplían la base legal sobre cómo deben realizarse las transferencias internacionales (ver artículo 23).

El Capítulo 3 incluye los derechos de los titulares de datos personales y las pautas básicas de su ejercicio. Los derechos que allí aparecen son el de acceso (ver artículo 27), el de rectificación (ver artículo 29), el de oposición (ver artículo 30) y el de supresión (ver artículo 31). Estos son los cuatro derechos básicos que le corresponden al titular de los datos y, aun con otras denominaciones o contenidos sensiblemente diferentes, aparecen tanto en la Ley vigente como en las regulaciones más actualizadas en la materia.

Respecto de estos derechos, las novedades más importantes aparecen en el derecho de oposición al tratamiento de datos y en el derecho de supresión de datos personales. Este último derecho engloba lo que en la actualidad se conoce como "derecho al olvido", denominación usualmente utilizada pero que ha traído muchas discusiones teóricas y críticas sobre su aplicación en la práctica, dado que una deficiente implementación podría devenir en violaciones a otros derechos fundamentales, como la libertad de expresión o el acceso a la información. De allí que en la propuesta que se somete a consideración, si bien

se reconoce este derecho, se ha aclarado especialmente que el derecho de supresión no procede cuando el tratamiento de datos persiga un fin público o sea necesario para ejercer el derecho a la libertad de expresión e información.

A esos cuatro derechos básicos se le ha agregado en este Capítulo, el derecho del titular de los datos a solicitar que sus datos personales se transfieran directamente de responsable a responsable cuando sea técnicamente posible –derecho a la portabilidad de datos personales– (ver artículo 33). Estos derechos no se encuentran en la legislación vigente, pero hallan reconocimiento en el derecho comparado y amplían el catálogo de derechos que se ponen a disposición para una mejor salvaguarda de los datos personales.

Este Capítulo concluye con reglas que determinan el modo para ejercer esos derechos (ver artículo 34), y algunas excepciones para hacerlo (ver artículo 36). Asimismo, la iniciativa adopta el criterio establecido por los artículos 9, 10 y 11 del Código Civil y Comercial de la Nación y expresamente dispone que el ejercicio abusivo de los derechos enumerados en el Capítulo no se encuentra amparado (ver artículo 35).

La novedad más importante que se incluye en el Capítulo 4, relacionada con las obligaciones de los responsables y encargados del tratamiento de datos, consiste en la enumeración de las acciones necesarias para el cumplimiento de la responsabilidad proactiva, tal como aparece definida en el Capítulo 1 y a la cual se hizo referencia anteriormente (ver artículo 37). Entre ellas, se destaca la obligación de adoptar políticas de privacidad o bien de adherirse a mecanismos de autorregulación vinculantes, tal como aparecen definidos en este mismo Capítulo.

Asimismo, se han incluido obligaciones que no están específicamente previstas en la Ley vigente, tales como la obligación de protección de datos desde el diseño y por defecto (ver artículo 38) y la obligación de realizar, en algunos casos de tratamiento de datos, una evaluación de su impacto en los datos personales (ver artículo 40).

Respecto de la primera, la propuesta legislativa la define básicamente como la obligatoriedad de aplicar medidas tecnológicas y organizativas apropiadas, tanto con anterioridad como durante el tratamiento de datos a fin de cumplir con los principios y los derechos de los titulares de los datos establecidos en la Ley. En relación con la protección por defecto, se entiende la aplicación de medidas similares a las anteriores, pero ahora con miras a garantizar que, por defecto, sólo sean objeto de tratamiento de datos aquellos datos personales que sean necesarios para cada uno de los fines del tratamiento. Finalmente, la evaluación de impacto está prevista en la propuesta solo en aquellos casos en los que un tratamiento pueda entrañar un alto riesgo de afectación a los derechos de los titulares en virtud de su naturaleza, alcance, contexto o finalidades (por ejemplo, el tratamiento de datos sensibles a gran escala).

Siguiendo la tendencia de varias legislaciones y a fin de facilitar el cumplimiento de la Ley, se crea la figura de un funcionario especializado, el Delegado de Protección de Datos (ver artículo 43), cuya designación será obligatoria para algunos casos específicamente definidos en la Ley (tratamiento de datos por parte de autoridades u organismos públicos; tratamiento de datos sensibles como parte de la actividad principal del responsable o encargado del tratamiento; y tratamiento de datos a gran escala). Sin perjuicio de que el espíritu de la Ley es impulsar una designación voluntaria de delegado, se ha optado por limitarlo a un número específico de situaciones en lugar de generalizarlo, dado los costos que ello podría acarrear a las empresas pequeñas o incluso a los particulares que hacen tratamiento de datos.

Resta aclarar que las funciones del delegado están previstas en la Ley proyectada (ver artículo 44), la cual también establece que ellas pueden ser desempeñadas por un empleado del responsable o encargado del tratamiento o en el marco de un contrato de locación de servicios. Con esta última pauta, sumado a que se establece que el Delegado de Protección de Datos podrá ejercer otras funciones siempre que no den lugar a conflictos de intereses, se pretende dar a los responsables y encargados una flexibilidad suficiente en la contratación para evitar costos significativos que puedan ser innecesarios.

El Capítulo 5 prevé la normativa que reemplazará a la vigente Ley Nº 26.951, a más de diez años de su sanción, pero que lamentablemente no ha alcanzado a cumplir con las expectativas creadas en la población.

Como surge de la versión del anteproyecto de ley disponible en el sitio web de la Agencia de Acceso a la Información Pública, la experiencia de la ex Dirección Nacional de Protección de Datos Personales ha demostrado que la regulación del Registro Nacional "No Llame" debería incorporarse al régimen general de protección de los datos personales, cuestión que ahora se hace mediante el Proyecto que se somete a consideración.

Sintéticamente, la propuesta propone la derogación de la mencionada Ley Nº 26.951 para incluir su objeto en este Proyecto (ver artículo 84). Se optó por seguir sus lineamientos adaptando su redacción al efecto de mejorar todo aquello relacionado con el ámbito del procedimiento para evaluar posibles infracciones. Especial atención se da a los montos de las multas que pueden imponerse: Además de adaptar los montos máximos de las multas a la nueva realidad económica, el Proyecto incluye la alternativa de determinar el valor de las multas hacia empresas utilizando con el valor del volumen de negocio total anual global facturado por la empresa en el ejercicio financiero anterior; ver artículo 69). La regulación proyectada también limita los recursos administrativos contra las resoluciones de la autoridad de control, que llevará a que el único recurso judicial sea, en caso de proceder, con efecto devolutivo, permitiendo así ejecutar prontamente las multas impuestas a los infractores (ver artículo 57). Asimismo, también se limitaron las excepciones vinculadas con el objeto del Proyecto (ver artículo 52), ya que la Ley vigente (ver artículo 8º de la Ley N° 26.951) contiene algunas que generan confusión: por ejemplo, se suprime la excepción concerniente a las llamadas vinculadas con campañas electorales, que nada tienen que ver con el objeto de la Ley.

Si bien es cierto que como se explicara previamente, este Proyecto elimina la obligación general de inscripción de bases de datos, para el caso de la implementación del Registro Nacional "No Llame", y tal como es en la

actualidad, se mantiene la obligación de registro de los sujetos obligados a consultar la lista de todos aquellos titulares o usuarios de líneas telefónicas que manifestaron su voluntad de no ser llamados con comunicaciones no deseadas (ver artículo 51). La implementación específica de este registro queda sujeta a la regulación que establezca la autoridad de control.

El Capítulo 6 hace referencia a cuatro supuestos especiales de tratamiento de datos personales. Ellos son las bases de datos públicas (ver artículo 58); el tratamiento de datos por organismos de seguridad e inteligencia (ver artículo 59); la prestación de servicios de información crediticia (ver artículo 60) y las bases destinadas a la publicidad (ver artículo 61). En este Capítulo se mantienen los lineamientos generales de la legislación vigente, aunque adaptada a las particularidades del Proyecto que se eleva a consideración. Las modificaciones que se han realizado tienden a un mejoramiento de algunas previsiones de la Ley vigente que estaban controvertidas por la jurisprudencia y parte de la doctrina especializada.

El Capítulo 7 hace referencia a la autoridad de control. Se designa a la Agencia de Acceso a la Información Pública (AAIP), conforme los términos del artículo 19 de la ley N° 27.275, sustituido por el artículo 11 del Decreto Nº 746/17, como la autoridad de control de la Ley Nº 25.326, siendo la AAIP un ente autárquico con autonomía funcional en el ámbito de la Jefatura de Gabinete de Ministros (ver artículo 62). Asimismo, se precisan con detalle sus facultades (ver artículo 63).

Este diseño institucional tiende a superar los problemas generados a raíz de las observaciones efectuadas por el Poder Ejecutivo Nacional ("veto parcial") de los puntos 2 y 3 del artículo 29 de la vigente Ley Nº 25.326 al momento de su promulgación, dispuesta con la salvedad de las partes observadas mediante el Decreto Nº 995 del 30 de octubre de 2000. A nivel internacional y nacional los problemas se pusieron de manifiesto como consecuencia de las observaciones que ocurrieron desde el momento mismo del nacimiento de la Ley vigente, dado que el veto mencionado restaba autonomía e independencia

a la autoridad de control, en contraposición a lo exigido por los estándares internacionales. Cabe notar que cuando la Unión Europea declaró a la República Argentina como país adecuado en materia de protección de datos personales realizó una observación sobre la independencia de la Dirección Nacional de Protección, en ese entonces dependiente del Ministerio de Justicia y Derechos Humanos, indicando que aquel diseño institucional debía ser reformado.

Por ello, este Proyecto mantiene el diseño institucional actual, que cumple con los estándares internacionales que requieren de autoridades de control cuya actuación esté dotada de garantías que permitan su independencia. En particular, es consistente con el artículo 1 del "Protocolo Adicional al Convenio para la Protección de las Personas con respecto al tratamiento automatizado de datos de carácter personal, a las autoridades de control y a los flujos transfronterizos de datos"; instrumento que forma parte del cuerpo normativo denominado Convenio 108 y del cual Argentina es Parte.

Finalmente, vale destacar que existen experiencias en el derecho comparado de organismos que unifican el acceso a la información pública y la protección de datos personales en una sola agencia, tal como ocurre en nuestra región con el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) de los Estados Unidos Mexicanos; o en Europa, con el Information Commissioner´s Office (ICO) del Reino Unido de Gran Bretaña e Irlanda del Norte.

El Capítulo 8 regula los procedimientos y las sanciones que podrá iniciar y, en su caso, aplicar la autoridad de control.

La regulación de los procedimientos resulta una novedad respecto de la normativa vigente, que carece de precisiones específicas como las que ahora se propone.

El Proyecto posibilita iniciar un procedimiento a instancias del titular de los datos o de su representante legal (ver artículo 65); un procedimiento de

verificación de oficio y un procedimiento de verificación por denuncia de un tercero (ver artículo 66).

Cabe destacar que el titular de los datos siempre tiene la posibilidad de hacer valer sus derechos ante la autoridad judicial competente, tal como se trata en el Capítulo siguiente. Ello no podría ser de otro modo ya que este Proyecto propicia una acción judicial de raigambre constitucional (la acción de habeas data) que no podría quedar supeditada a la tramitación de un reclamo administrativo previo. Sin embargo, y a fin de evitar posibles conflictos, se dispone que el titular de los datos no pueda iniciar el reclamo administrativo previsto en el Capítulo 8, si ya ha iniciado la acción judicial (ver artículo 34). Queda claro que, en caso de haberla iniciado, al tomar conocimiento de ello la autoridad de control deberá suspender el trámite previsto en este Capítulo.

De todos modos, el Proyecto alienta la presentación de denuncias ante la autoridad de control, disponiendo, en todos los casos, de instancias de conciliación (ver artículo 64). Éstas pueden resultar en beneficio no solo de los titulares de los datos para obtener satisfacción a sus reclamos, sino también de los responsables del tratamiento de datos, que podrán contar con una instancia de acuerdo con quien se siente afectado, a fin de solucionar el conflicto sin activar la instancia judicial. Por lo demás, en caso de no haber conciliación, la autoridad de control puede indicar el cumplimiento del derecho o los derechos vulnerados (ver artículo 67) y aplicar las sanciones correspondientes (ver artículo 69), para cuyo eventual examen se prevé un recurso judicial ante la Cámara Nacional de Apelaciones en lo Contencioso Administrativo Federal de la Capital Federal (ver artículo 68).

En relación con las sanciones, el Proyecto innova respecto de la regulación actual al permitir la posibilidad que las multas sean cuantificadas en base a una referencia de valor (un porcentaje del valor del volumen de negocio total anual global facturado por la empresa en el ejercicio financiero anterior) que permite superar las dificultades que surgen de la insuficiencia de los montos contenidos en la legislación vigente, en atención a que los daños que se pueden ocasionar

por infracción a la Ley configuran lesiones a derechos fundamentales, como la privacidad o la intimidad (ver artículo 69).

Es de notar que la multa no es la única sanción que puede imponer la autoridad de control de acuerdo con el Proyecto. Por ser una autoridad de control que goza de independencia, se la faculta a imponer otras sanciones, algunas de las cuales ya están previstas en la legislación vigente. Entre ellas, se encuentran la suspensión y el cierre de actividades de tratamientos de datos, incluida la posibilidad que, de manera temporal o definitiva, se retire, bloquee o suspenda el acceso a determinados datos personales a los que los responsables del tratamiento den acceso. Con estas facultades, que deberán ser ejercidas con la máxima prudencia ante la posible vulneración de otros derechos fundamentales, como el acceso a la información o el ejercicio de la libertad de expresión, el Proyecto sigue la normativa propuesta en el citado "Reglamento (UE) 2016/679", entre otros ejemplos del derecho comparado.

El Capítulo 9 reglamenta específicamente la acción judicial de habeas data. Sin perjuicio de las adaptaciones terminológicas que fueron necesarias realizar a efectos de compatibilizar la acción con el Proyecto en su totalidad, la mayor innovación consistió en la ampliación de la legitimación activa (ver artículo 72).

En relación con la competencia, no obstante algunas posiciones en contrario, se decidió mantener el criterio sustentado por la Corte Suprema de Justicia de la Nación y asignar el conocimiento y decisión de estos casos a la jurisdicción federal (ver artículo 68).

Finalmente, en los Capítulos 10 y 11 se han incluido, respectivamente, disposiciones transitorias y finales vinculadas a los plazos establecidos para el desarrollo de la estructura de la autoridad de control y las previsiones presupuestarias que serán necesarias.

Se dispone, asimismo, un plazo de reglamentación de 180 días que se estima necesario, dados los cambios que propone el Proyecto respecto de la legislación vigente. La entrada en vigencia de la Ley está prevista a los dos (2)

años de su publicación oficial –es decir con posterioridad a su reglamentación–; también se establece que durante el mismo plazo los responsables y encargados del tratamiento de datos deberán adaptarse a las nuevas regulaciones.

En el Capítulo relacionado a las disposiciones finales, se ha decidido mantener la regulación vigente sobre la jurisdicción y se derogan expresamente las Leyes Nros. 25.326, 26.343 y 26.951.

Por todo lo expuesto, y con el convencimiento de que la presente iniciativa legislativa constituye un avance para nuestro país en materia de protección de los datos personales, les solicitamos a nuestros colegas que acompañen favorablemente esta iniciativa.

Autora:

BANFI, Karina