LEY DE PROTECCIÓN DE LOS DATOS PERSONALES

EL SENADO Y CÁMARA DE DIPUTADOS

DE LA NACIÓN ARGENTINA REUNIDOS EN CONGRESO...

SANCIONAN CON FUERZA DE

LEY

Capítulo I

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.

ARTÍCULO 2° - (Definiciones).

1. A los fines de la presente ley se entiende por:

- Autoridad de control: Órgano de control que debe velar por el cumplimiento de los principios y procedimientos de la presente ley de acuerdo a lo establecido en el Capítulo VII.

- 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.

- Cesión: Toda transmisión de datos realizada a persona distinta del titular de los datos, del responsable o del encargado del tratamiento que implique que el cesionario pueda realizar tratamiento ulterior de esos datos a su arbitrio.

- Computación en la nube: Modelo en el cual un tercero brinda capacidad de infraestructura, plataformas o servicios de software para habilitar acceso conveniente por demanda a un conjunto compartido de recursos computacionales configurables, por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios, que pueden ser rápidamente aprovisionados y liberados con un esfuerzo mínimo de administración o de interacción con el proveedor de servicios.

- Datos biométricos: Datos personales 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.

- Datos genéticos: Datos personales relativos a las características genéticas heredadas o adquiridas de una persona humana que proporcionen una información sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.

- Datos personales: Información de cualquier tipo referida a personas físicas determinadas o determinables, inclusive los datos biométricos. Se entenderá por determinable la persona que pueda ser identificada, directa o indirectamente, 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.

- 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, información referente a la salud o preferencia 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 debería 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.

- 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, y en su caso, accesible sin otro requisito más que el pago de una contraprestación.

- Fuente de acceso público: 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.

- Fuente de acceso restringido: Aquella que contiene información afectada por el secreto profesional o por la confidencialidad impuesta legalmente.

- 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.

- 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.

- Servicios de telefonía: 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.

- Servicios de la sociedad de la información: Servicios prestados a distancia, por vía electrónica, a petición individual del destinatario y generalmente a título oneroso. Comprenden los servicios prestados a través de Internet siempre que representen una actividad económica para el prestador.

- Tercero: La persona humana o jurídica, distinta del titular de los datos, del responsable del tratamiento o del encargado del tratamiento.

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

- Transferencia internacional: Implica 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, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

- Vulneración de seguridad de datos personales: Cualquier incidente 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.

ARTÍCULO 3° - (Excepciones).

1. 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.

2. La aplicación de la presente ley en ningún caso podrá afectar el secreto de las fuentes de información periodísticas.

ARTÍCULO 4° - (Ámbito de aplicación).

1. Las normas de la presente ley serán de aplicación cuando:

a) El responsable del tratamiento se encuentre radicado 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 II

Principios relativos al tratamiento de datos

ARTÍCULO 5º - (Principio de licitud, lealtad y transparencia).

Los datos personales serán tratados de manera lícita, leal y transparente en relación con el titular de los datos.

ARTÍCULO 6º - (Principio de finalidad).

1. Los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.

2. 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 también el tratamiento de datos con fines que pudieron ser, de acuerdo al contexto, razonablemente presumidos por el titular de los datos y no fuesen perjudiciales para sus intereses.

ARTÍCULO 7º - (Principio de minimización de datos).

Los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

ARTÍCULO 8º - (Principio de exactitud).

Los datos personales serán exactos y completos. Si fuera necesario adecuarlos, se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación.

ARTÍCULO 9º - (Limitación del plazo de conservación).

Los datos personales serán mantenidos de forma que se permita la identificación de los titulares de los datos durante no más tiempo del necesario para los fines del tratamiento de datos. Los datos personales podrán conservarse durante períodos más largos siempre que se traten 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 deberá 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).

1. El tratamiento de datos sólo será lícito si se cumple al menos una 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 es 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 que requieran la protección de datos personales, en particular cuando el titular sea un niño, niña o adolescente.

2. Lo dispuesto en el apartado b) del inciso 1 no será de aplicación al tratamiento de datos realizado por las autoridades públicas en el ejercicio de sus funciones.

ARTÍCULO 12. - (Consentimiento).

1. El tratamiento de datos, en cualquiera de sus formas, requiere del consentimiento de su titular para una o varias finalidades específicas, salvo lo previsto en el art. 11 inciso 1 apartado b).

2. El consentimiento podrá ser obtenido de forma expresa o tácita.

La forma del consentimiento dependerá 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, podrá 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 requerirá el consentimiento expreso, salvo las excepciones establecidas por ley.

El consentimiento tácito será 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. Será 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 deberá ser compatible con las finalidades manifiestas que surgen del contexto que originó la recolección. En ningún caso procederá para el tratamiento de datos sensibles.

3. En todos los casos, el responsable del tratamiento tendrá la carga de demostrar que el titular de los datos consintió el uso de sus datos personales.

ARTÍCULO 13. - (Revocación del consentimiento).

1. El consentimiento podrá ser revocado en cualquier momento. Dicha revocación no tendrá 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.

2. El responsable del tratamiento debe informar al titular de los datos, previo a su recolección y durante el tratamiento, las consecuencias que tendrá una eventual revocación.

ARTÍCULO 14. - (Excepciones al consentimiento previo).

1. No será necesario el consentimiento para el tratamiento de datos cuando:

a) Los datos figuren en fuentes de acceso público irrestricto;

b) Se recaben para el ejercicio de funciones propias de los poderes del Estado y sean necesarios para el cumplimiento estricto de sus competencias;

c) Se obtengan en virtud de una obligación que proviene de una ley;

d) Deriven de una relación jurídica entre el titular de los datos y el responsable del tratamiento, y resulten necesarios para su desarrollo o cumplimiento;

e) Cuando resulten necesarios 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.

ARTÍCULO 15. - (Información al titular de los datos).

1. El responsable del tratamiento deberá brindar al titular de los datos antes de la recolección y durante el tratamiento de los datos, 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 y, en su caso, del delegado de protección de datos;

c) Los medios para ejercer los derechos de acceso, rectificación, supresión y oposición de conformidad con lo dispuesto en esta Ley;

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

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

f) El derecho a presentar una denuncia ante la autoridad de control o a ejercer la acción de habeas data en caso de que el responsable del tratamiento incumpla con la presente ley.

2. Cuando los datos personales no se hayan obtenido directamente de su titular, el responsable del tratamiento quedará eximido de brindar la información prevista en el inciso precedente cuando ello resulte imposible o suponga un esfuerzo desproporcionado.

ARTÍCULO 16. - (Tratamiento de datos sensibles).

1. 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 que por ley no sea requerido el otorgamiento de dicha autorización;

b) El tratamiento 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) El tratamiento sea efectuado por los establecimientos sanitarios públicos o privados y los profesionales vinculados a la ciencia de la salud que traten los datos recogidos de fuentes de acceso restringido o los datos de los pacientes que estén o hubieran estado bajo tratamiento de aquellos, respetando los principios del secreto profesional.

d) El tratamiento sea efectuado en el curso 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 a las personas que mantengan un contacto regular por razón de su objeto principal.

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

f) El tratamiento tenga una finalidad histórica, estadística o científica. En este caso, deberá adoptarse un procedimiento de disociación de datos.

ARTÍCULO 17. - (Tratamiento de antecedentes penales y contravencionales).

1. 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.

2. El empleador que conserve un certificado, documento o información de antecedentes penales o contravencionales de sus empleados no podrá cederlo a terceros, salvo con el consentimiento del titular de los datos.

ARTÍCULO 18. — (Tratamiento de datos de menores).

1. En el tratamiento de datos concernientes a un niño, niña o adolescente, se deberá 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.

2. Se considerará 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 y aptos para ellos. En estos casos, el consentimiento se considerará lícito cuando el niño, niña o adolescente tenga como mínimo trece (13) años. Si el niño es menor de trece (13) años, tal tratamiento únicamente se considerará lícito si el consentimiento lo otorgó el titular de la responsabilidad parental o tutela sobre el niño, y solo en la medida en que se dio o autorizó.

3. El responsable del tratamiento deberá realizar esfuerzos razonables para verificar en tales casos que el consentimiento fue 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).

1. El responsable del tratamiento y, en su caso, el encargado deberán 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.

2. El responsable del tratamiento adoptará 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 una vulneración para los titulares de los datos;

e) Las vulnerabilidades previas ocurridas en los sistemas de tratamiento;

f) El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada a su posesión.

ARTÍCULO 20. - (Notificación de incidentes de seguridad).

1. El responsable del tratamiento deberá informar a la autoridad de control en un tiempo razonable, atendiendo a las circunstancias del caso, las vulneraciones de seguridad de datos personales ocurridas en cualquier fase del tratamiento de datos que afecten de forma significativa derechos de titulares de los datos, en cuanto confirme que ocurrió la vulneración y haya tomado las medidas necesarias para iniciar un proceso de revisión exhaustiva de la magnitud de la afectación.

2. De igual manera, el responsable del tratamiento también deberá informar al titular de los datos la vulneración de seguridad ocurrida, en un lenguaje claro y sencillo.

3. La notificación a que se refieren los incisos anteriores deberá contener, al menos, la siguiente información:

a) La naturaleza del incidente;

b) Los datos personales 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.

4. El responsable del tratamiento deberá documentar toda vulneración de seguridad de los datos personales ocurrida en cualquier fase del tratamiento de datos, identificando, de manera enunciativa pero no limitativa, la fecha en que ocurrió, el motivo de la vulneración, los hechos relacionados con ella y sus efectos, y las medidas correctivas implementadas de forma inmediata y definitiva.

ARTÍCULO 21. - (Deber de confidencialidad).

1. 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 subsistirá aun después de finalizada su relación con el titular de los datos, el responsable o el encargado del tratamiento, según corresponda.

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

ARTÍCULO 22. - (Cesión).

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

El consentimiento para la cesión es revocable.

2. El consentimiento no es exigido cuando la cesión:

a) Se encuentre prevista en una ley o tratado en los que la República Argentina sea parte;

b) Involucre mínimamente datos recogidos de fuentes de acceso público irrestricto;

c) Se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias;

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

e) Resulte necesaria para el desarrollo o cumplimiento de una relación jurídica entre el titular de los datos y el responsable del tratamiento;

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

g) Hubiera aplicado un procedimiento de disociación de datos;

h) 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.

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

ARTÍCULO 23. - (Transferencia internacional).

1. Toda transferencia internacional de datos personales para ser lícita, deberá contar con el consentimiento de su titular.

2. El consentimiento del titular de los datos no será requerido en los siguientes supuestos:

a) Cuando la transferencia internacional esté prevista en una ley o tratado en los que la República Argentina sea parte;

b) Cuando la transferencia internacional sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios;

c) Cuando la transferencia internacional 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;

d) Cuando la transferencia internacional 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;

e) Cuando la transferencia internacional sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia;

f) Cuando la transferencia internacional sea necesaria para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial;

g) Cuando la transferencia internacional sea necesaria para el mantenimiento o cumplimiento de una relación jurídica entre el responsable del tratamiento y el titular de los datos.

h) Cuando la transferencia internacional sea requerida para los supuestos previstos en el art. 24 inciso 2 apartados c) y e).

3. El receptor de los datos personales asumirá las mismas obligaciones que corresponden al responsable del tratamiento que transfirió los datos personales.

ARTÍCULO 24. - (Carácter adecuado del país u organismo receptor).

1. La transferencia internacional de datos personales de cualquier tipo sólo podrá realizarse a países u organismos internacionales o supranacionales, que proporcionen niveles de protección adecuados.

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 de que se trate, así como las normas profesionales, códigos de conducta y las medidas de seguridad en vigor en dichos lugares, o que resulten aplicables a los organismos internacionales o supranacionales.

2. La prohibición de transferencia internacional de datos a países u organismos no adecuados no regirá en los siguientes supuestos:

a) Colaboración judicial internacional;

b) Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica. En este último caso se deberá aplicar un proceso de disociación de datos;

c) Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable;

d) Cuando la transferencia internacional se hubiera acordado en el marco de tratados internacionales en los cuales la República Argentina sea parte;

e) Cuando la transferencia internacional 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;

f) Cuando el titular de los datos hubiera consentido expresamente la transferencia internacional, previa información del carácter no adecuado del país u organismo internacional o supranacional receptor.

g) Cuando el responsable del tratamiento transferente y el destinatario adopten mecanismos de autorregulación vinculante, siempre y cuando éstos sean acorde a las disposiciones previstas en esta ley.

h) Cuando la transferencia internacional se realice al amparo que establezcan las cláusulas contractuales que prevean la protección de datos personales acordes con las disposiciones de la presente ley.

ARTÍCULO 25. - (Prueba del cumplimiento de las obligaciones en materia de transferencias internacionales).

A efectos de demostrar que la transferencia internacional se realizó conforme a lo que establece la presente ley, la carga de la prueba recaerá, en todos los casos, en el responsable del tratamiento que transfiere.

ARTÍCULO 26. - (Tratamiento de datos que utilizan servicios de computación en la nube).

1. El tratamiento de datos que utilizan servicios de computación en la nube estará permitido cuando se garantice el cumplimiento de los principios y obligaciones establecidos por la presente ley.

2. El responsable del tratamiento debe elegir un proveedor de servicios que garantice el cumplimiento de la presente ley y responderá solidariamente ante el titular de los datos y ante la autoridad de control por incumplimientos del proveedor.

En especial, el responsable del tratamiento deberá controlar que el proveedor del servicio de computación en la nube:

a) Cuente con una política de protección de datos personales o condiciones de servicio en los que se detallen las medidas dispuestas para garantizar la protección de los datos

personales, y que su aplicación sea efectiva. Debe 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 las 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.

3. Las condiciones en las que se brinda el servicio de computación en la nube deberán:

a) Permitir que el responsable del tratamiento pueda limitar el tipo de tratamiento de datos sobre los que presta el servicio;

b) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que presta el servicio;

c) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable del tratamiento y que este último los haya podido recuperar;

d) Impedir el acceso a los datos personales a quienes no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud de autoridad competente, informar de ese hecho al responsable del tratamiento.

Capítulo III

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, así como a conocer cualquier información relacionada con las condiciones generales y específicas de su tratamiento.

ARTÍCULO 28. - (Contenido de la información).

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

a) Los fines 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 serán cedidos los datos personales, en particular destinatarios de transferencias internacionales de datos;

d) De ser posible, el plazo previsto de conservación de los datos personales o, de no ser 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;

f) El derecho a presentar una denuncia 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, así como la importancia y las consecuencias previstas de dicho tratamiento para el titular de los datos.

2. La información debe ser amplia y versar sobre la totalidad del registro perteneciente al titular de los datos, aun cuando el requerimiento sólo comprenda un aspecto de los datos personales. En ningún caso el informe podrá revelar datos pertenecientes a terceros, aun cuando se vinculen con el titular de los datos.

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

ARTÍCULO 29. - (Derecho de rectificación).

1. 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.

2. 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 día hábil de efectuada.

3. Durante el proceso de verificación y rectificación del error o falsedad de la información que se trate, el responsable del tratamiento deberá o bien bloquear el dato, o consignar al proveer información relativa al mismo la circunstancia de que se encuentra sometida a revisión.

ARTÍCULO 30. - (Derecho de oposición).

1. El titular de los datos podrá oponerse al tratamiento de sus datos, o de una finalidad específica del mismo, cuando no hubiera prestado consentimiento y existan motivos fundados y legítimos relativos a una concreta situación personal.

2. La oposición procederá cuando:

a) El tratamiento de datos no se encuentre fundado en una autorización legal.

b) Los datos personales sean objeto de un tratamiento automatizado en los términos del artículo 32, el cual le produzca efectos jurídicos no deseados o afecte de manera significativa sus intereses, derechos o libertades, y estén destinados a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.

c) El tratamiento de datos tenga por objeto la publicidad, venta directa y otras actividades análogas, incluida la elaboración de perfiles.

ARTÍCULO 31. - (Derecho de supresión).

1. El titular de los datos tendrá derecho a solicitar la supresión de sus datos personales de las bases de datos y sistemas 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.

2. La supresión procederá cuando:

a) Los datos personales ya no sean necesarios en relación con los fines para los que fueron recolectados o tratados de otro modo;

b) El titular de los datos retire 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 el 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.

3. La supresión no procederá cuando:

a) Pudiese causar perjuicios a derechos o intereses legítimos de terceros;

b) Prevalezcan razones de interés público para el tratamiento de datos;

c) 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.

4. La supresión tampoco procederá cuando el tratamiento de datos sea necesario para ejercer el derecho a la libertad de expresión e información.

ARTÍCULO 32. - (Valoraciones personales automatizadas).

1. El titular de los datos tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento de datos automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

2. El titular de los datos no podrá ejercer el derecho referido en el inciso anterior si la decisión:

a) Es necesaria para la celebración o la ejecución de un contrato entre el titular de los datos y un responsable del tratamiento;

b) Está autorizada por ley;

c) Se basa en su consentimiento expreso.

3. En los casos a que se refieren los apartados a) y c) del inciso 2, el responsable del tratamiento adoptará 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).

1. Cuando se brinden servicios en forma electrónica que incluyan el tratamiento de datos personales, el titular de los datos tendrá 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 podrá solicitar que sus datos personales se transfieran directamente de responsable a responsable cuando sea técnicamente posible.

2. 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).

1. El ejercicio de cualquiera de los derechos del titular de los datos no es requisito previo, ni impide el ejercicio de otro.

2. 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 64 o, a elección del titular de los datos, podrá interponer la acción de habeas data prevista en el artículo 69 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.

3. 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 le corresponderá a sus sucesores universales.

4. El responsable del tratamiento deberá establecer medios y procedimientos sencillos, expeditos, accesibles y gratuitos que permitan al titular de los datos ejercer sus derechos de acceso, rectificación, oposición y supresión al tratamiento de sus datos personales.

5. 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 un interés legítimo al efecto.

ARTÍCULO 35. - (Abuso de derecho).

El ejercicio abusivo de los derechos enumerados en los artículos precedentes 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).

1. Los responsables del tratamiento de bases de datos públicas pueden, mediante decisión fundada, denegar el acceso, rectificación, la oposición o la supresión 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.

2. 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 afectado.

3. En cualquier caso el responsable del tratamiento deberá 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 IV

Obligaciones de los responsables y encargados del tratamiento

ARTÍCULO 37. - (Medidas para el cumplimiento de la responsabilidad proactiva).

1. Las medidas adoptadas para el cumplimiento de las disposiciones de la presente ley deberán 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 tener sobre los derechos del titular de los datos.

2. Deberán 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.

3. Las medidas deberán ser aplicadas de manera tal que permitan su demostración ante el requerimiento de la autoridad de control.

4. Se deberá 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.

5. La verificación de estas medidas por parte de la autoridad de control será tenida en cuenta al momento de evaluar la imposición de sanciones por incumplimientos a la presente, conforme el procedimiento previsto por el artículo 65.

ARTÍCULO 38. - (Protección de datos desde el diseño y por defecto).

1. El responsable del tratamiento aplicará 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 serán 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.

2. El responsable del tratamiento aplicará las medidas tecnológicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento de datos aquellos datos personales que sean necesarios para cada uno de los fines del tratamiento. Esta obligación se aplicará 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 garantizarán en particular que, por defecto, los datos

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

ARTÍCULO 39. - (Tratamiento de datos por cuenta de terceros).

1. La prestación de servicios de tratamiento de datos por cuenta de terceros, entre un responsable y un encargado del tratamiento deberá quedar formalizada mediante un contrato. 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 podrán aplicarse o utilizarse con un fin distinto al que figure en el contrato, ni cederlos a otras personas, ni aun para su conservación, salvo autorización expresa del responsable del tratamiento.

El contrato previsto en el párrafo anterior deberá 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, así como las obligaciones y responsabilidades del responsable y encargado del tratamiento.

2. Una vez cumplida la prestación contractual, los datos personales tratados deberán ser destruidos, salvo que medie autorización expresa del encargado o cuando se hubiera previsto en el contrato que razonablemente se puede presumir la posibilidad de ulteriores encargos, en cuyo caso se podrá almacenar los datos personales con las debidas condiciones de seguridad por un período de hasta dos (2) años.

3. El encargado podrá 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 asumirá el carácter de encargado en los términos y condiciones previstos en esta ley. Para el supuesto 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.

ARTÍCULO 40.- (Evaluación de impacto relativa a la protección de datos personales).

1. Cuando el responsable del tratamiento pretenda llevar a cabo un tipo de tratamiento de datos que por su naturaleza, alcance, contexto o finalidades, sea probable que entrañe un alto riesgo de afectación de derechos fundamentales de los titulares de los datos, deberá realizar, de manera previa a la implementación del tratamiento, una evaluación del impacto en la protección de los datos personales.

2. La evaluación de impacto relativa a la protección de los datos será 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 físicas 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 físicas 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;

c) Tratamiento de datos mediante tecnologías que se consideren potencialmente invasivas de la privacidad, como la observación sistemática a gran escala de una zona de acceso público (videovigilancia), la utilización de aeronaves no tripuladas (*drones*), la vigilancia electrónica, la minería de datos, la geolocalización, el tratamientos de datos a gran escala, la denominada "Internet de las Cosas"; entre otras;

d) Tratamiento significativo no incidental de datos de niñas, niños y adolescentes, o dirigido especialmente a tratar datos de los mismos.

ARTÍCULO 41. - (Contenido de la evaluación de impacto).

1. La evaluación deberá 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 apartado a);

d) Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con la presente ley, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

ARTÍCULO 42. - (Informe previo).

1. El responsable del tratamiento informará 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.

2. El informe a la autoridad de control con arreglo al inciso 1 incluirá, como mínimo, la siguiente información:

a) En su caso, las responsabilidades respectivas del responsable del tratamiento, los corresponsables 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 los interesados 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;

f) Cualquier otra información que solicite la autoridad de control.

3. Cuando la autoridad de control considere que el tratamiento de datos previsto a que se refiere el inciso 1 pueda infringir la presente ley, intimará al responsable del tratamiento, o en su caso, al encargado, a que arbitre las medidas necesarias a los fines de su subsanación y en su caso, suspenda el tratamiento.

ARTÍCULO 43. - (Delegado de Protección de Datos).

1. Los responsables y encargados del tratamiento deberán designar un delegado de protección de datos en algunos de los siguientes supuestos:

a) Se trate 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.

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 inciso, pero decidan designarlo 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 siguiente.

2. Cuando se trate de una autoridad u organismo público con dependencias subordinadas, se podrá designar un único delegado de protección de datos, teniendo en consideración su tamaño y estructura organizativa.

3. Un grupo económico podrá nombrar un único delegado de protección de datos siempre que esté en contacto permanente con cada establecimiento.

4. La designación del delegado de protección de datos deberá recaer en una persona que reúna los requisitos de idoneidad, capacidad y conocimientos específicos para el ejercicio de sus funciones.

5. Las funciones de delegado de protección de datos podrán 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 podrá ejercer otras funciones siempre que no den lugar a conflictos de intereses.

6. En cualquier caso, el delegado ejercerá sus funciones sin recibir instrucciones y sólo responderá ante el más alto nivel jerárquico de la organización.

ARTÍCULO 44. - (Funciones del delegado de protección de datos).

El delegado de protección de datos tendrá, al menos, las siguientes funciones:

a) Informar y asesorar a los responsables y encargados del tratamiento (y 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 dicha normativa y de la política de protección de datos de un organismo público, empresa o entidad privada: asignación de responsabilidades, concienciación y formación del personal, y las auditorías correspondientes;

d) Ofrecer el asesoramiento que se le solicite para hacer la evaluación de impacto de un tratamiento de datos, cuando entrañe un alto riesgo para los derechos y libertades de las personas físicas, y supervisar luego su aplicación;

e) 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).

1. 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.

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

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

4. En el mismo sentido, 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.

5. Los mecanismos de autorregulación vinculantes serán presentados a la homologación de la autoridad de control, la cual dictaminará si el proyecto es conforme con la presente ley y, en su caso, aprobará el ordenamiento o indicará las correcciones que se estime necesarias para su aprobación.

6. Los mecanismos de autorregulación vinculantes que resulten aprobados de conformidad con el inciso precedente, serán registrados y dados a publicidad por la autoridad de control.

Capítulo V

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)

1. El objeto del registro establecido por el artículo precedente 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.

2. Las situaciones contempladas y reguladas por el presente capítulo se deben interpretar en todos los casos teniendo en cuenta el requerimiento del titular o usuario.

ARTÍCULO 48. - (Servicios de telefonía)

1. La autoridad de control podrá individualizar e incorporar, dentro de las modalidades de servicios de telefonía, a aquellos nuevos servicios que la tecnología ofrezca en el futuro y sean compatibles con el objeto del Registro Nacional “No Llame”.

ARTÍCULO 49. - (Inscripción)

1. Podrá inscribirse en el Registro Nacional “No Llame” toda persona humana titular o usuario autorizado del servicio de telefonía en cualquiera de sus modalidades que manifieste su voluntad de no ser contactada por quien publicitare, ofertare, vendiere o regalare bienes o servicios, sin perjuicio de lo dispuesto en el artículo 60 de la presente ley.

ARTÍCULO 50. - (Gratuidad y simplicidad)

1. 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 solo podrán ser realizados por el titular o usuario de la línea telefónica.

2. La baja sólo puede ser solicitada por el titular o usuario en cualquier momento y tendrá efectos inmediatos.

ARTÍCULO 51. - (Sujetos Obligados e Inscripción)

1. 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.

2. 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 la misma, resultando aplicables, en el caso de corresponder, las previsiones del artículo 22 inc. 3.

3. Los sujetos obligados que contraten campañas en el exterior deberán 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.

4. Será considerado 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 incisos precedentes.

5. Los sujetos obligados no podrán dirigirse a ninguno de los inscriptos en el Registro Nacional “No Llame”.

6. Quienes realicen efectivamente el contacto telefónico deberán:

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 párrafo anterior. La autoridad de control establecerá el procedimiento para esa inscripción.

7. En caso de duda, deberá interpretarse que no corresponde el contacto telefónico con quien se hubiera inscripto en el Registro Nacional “No Llame”.

ARTÍCULO 52. - (Excepciones)

1. Quedan exceptuadas de la presente ley:

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, inscriptos en el Registro Nacional “No Llame”.

ARTÍCULO 53. - (Condiciones de contacto)

1. Los contactos telefónicos de publicidad, oferta, venta y regalo de bienes o servicios no solicitados deberán realizarse desde un número visible por el identificador de llamadas u otra tecnología que posea el titular o usuario de la línea telefónica.

2. 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 precedente, deben ser realizadas en forma y horario razonables y de acuerdo a la reglamentación.

ARTÍCULO 54. - (Denuncias)

El titular o usuario autorizado del servicio de telefonía en cualquiera de sus modalidades podrá realizar la denuncia por incumplimiento del presente capítulo ante la autoridad de control dentro de un 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 64 inciso 3. Verificada la existencia de la infracción, quienes la hayan cometido serán pasibles de las sanciones previstas en el artículo 68.

ARTÍCULO 56. - (Recepción de Prueba y Resolución)

1. 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.

2. A requerimiento de la autoridad de control, los sujetos obligados deberán brindar, en el plazo que se disponga, el registro de sus llamadas salientes provisto por la empresa prestadora del servicio de telecomunicaciones de la que fueran usuarios, quien deberá proveerlo en un plazo máximo de diez (10) días y en las condiciones que la autoridad de control disponga.

3. 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.

4. El incumplimiento de la requisitoria a que se refieren los incisos 2 y 3 hará pasibles a las empresas prestadoras del servicio de telecomunicaciones de las sanciones previstas en el artículo 68 inciso 2 apartado b).

5. 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.

6. La resolución de la autoridad de control podrá:

a) Archivar la denuncia.

b) Imponer una sanción en caso que se hubiera verificado el incumplimiento a la presente ley.

7. La resolución de la autoridad de control mencionada en el apartado b) del inciso anterior agotará la vía administrativa a los efectos de lo previsto en la Ley Nacional de Procedimientos Administrativos Nº 19.549. 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 VI

Supuestos especiales

ARTÍCULO 57. - (Bases de datos públicas).

1. La creación, modificación o supresión de bases de datos pertenecientes a autoridades u organismos públicos debe hacerse por medio de disposición general.

2. Las disposiciones respectivas, deben indicar:

a) Órganos responsables del archivo, 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 de acceso, rectificación, supresión u oposición.

3. En las disposiciones que se dicten para la supresión de las bases se establecerá el destino de las mismas o las medidas que se adopten para su destrucción.

ARTÍCULO 58.- (Tratamiento de datos por organismos de seguridad e inteligencia).

1. 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 Congreso de la

Nación y la Comisión de Defensa Nacional de la Cámara de Senadores de la Nación, o las que las sustituyan, tendrán acceso a las bases de datos mencionadas en este inciso por razones fundadas y en aquellos aspectos que constituyan materia de competencia de tales comisiones.

2. 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 inteligencia, cuando sea necesario realizar sin el consentimiento del titular, quedará 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.

3. Se suprimirán, aún si no mediare solicitud del titular, los datos personales de las bases de datos mencionadas en el inciso 1 cuando no sean necesarios para los fines que motivaron su recolección. La supresión se realizará por resolución fundada de la autoridad competente dentro de un plazo razonable.

ARTÍCULO 59. - (Prestación de servicios de información crediticia).

1. 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 accesibles al público o procedentes de informaciones facilitadas por el interesado o con su consentimiento.

2. 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.

3. A solicitud del titular de los datos, el responsable o encargado del tratamiento le comunicará en forma gratuita las informaciones, evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos doce (12) meses y el nombre y domicilio del cesionario en el supuesto de tratarse de datos obtenidos por cesión.

4. Sólo se podrán 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. El plazo se reducirá a un (1) año cuando el deudor cancele o extinga la obligación. 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 financieras según normativa del Banco Central de la República Argentina;

c) El inicio de la acción judicial de cobro;

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

e) Para las deudas verificadas o en trámite de verificación en los procesos de concursos preventivos y quiebras, se tomará como última fecha significativa a los fines de computar el plazo de cinco (5) años, la fecha de la apertura del concurso de acreedores o de la declaración de quiebra, respectivamente;

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

5. La prestación de servicios de información crediticia no requerirá el previo consentimiento del titular de los datos a los efectos de su cesión, ni la ulterior comunicación de ésta, cuando estén relacionados con el giro de las actividades comerciales o crediticias de los cesionarios.

6. 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 deberán enviar al titular de los datos, al último domicilio por él denunciado, una notificación fehaciente en la que se le comunique la información a ceder y sus cesionarios. En caso de disconformidad con el contenido de la información a ceder, el titular de los datos podrá ejercer los derechos que le otorga esta ley. Una vez cursada dicha notificación al titular de los datos, no se requiere nueva notificación para otras cesiones referidas a la misma obligación. La información podrá ser difundida por las empresas que prestan servicios de informes crediticios luego de transcurridos diez (10) días hábiles de cursada aquella notificación. Si el titular de los dato cumple su obligación dentro de los cinco (5) días hábiles de notificado, no podrán cederse tales datos a las empresas que prestan servicios de informe crediticio.

7. Los tratamientos de datos efectuados por el Estado quedan exceptuados de la notificación dispuesta en el inciso precedente.

8. Las entidades financieras que obligatoriamente cedan información relativa al cumplimiento de obligaciones de contenido patrimonial al Banco Central de la República Argentina, deberán cursar una notificación fehaciente al titular de los datos, al último domicilio por él denunciado, informándole sobre su calificación de incumplimiento y sus cesionarios. Esta notificación se realizará cuando las obligaciones pasen de cumplimiento normal a incumplimiento, sin que se deba notificar la continuidad de tal incumplimiento y/o el agravamiento de la calificación. Esta notificación se realizará dentro de los diez (10) días hábiles de producida esta nueva calificación y con independencia de la eventual cesión de los datos al Banco Central de la República Argentina. El titular de los datos, en caso de disconformidad con el contenido de la información notificada, podrá ejercer los derechos que le otorga esta ley. Si el titular de los datos cumple dicha obligación dentro de los cinco (5) días hábiles de notificado, tales datos no podrán cederse a las empresas que prestan servicios de informe crediticio, ni ser difundidos al público por el Banco Central de la República Argentina.

9. Cuando se denegare 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 del mismo.

10. Se deberán suprimir los datos personales de los fiadores o avalistas cuando se haya cancelado o extinguido la obligación, debiendo el titular de los datos acreditar ante la empresa de informes crediticios dicha cancelación o extinción de la deuda, en la modalidad y plazos dispuestos por el artículo 34 de la presente ley.

ARTÍCULO 60. - (Bases destinadas a la publicidad).

1. Podrán tratarse sin consentimiento de su titular datos con fines de publicidad, venta directa y otras actividades análogas, cuando estén destinados a la formación de perfiles determinados, 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.

2. 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, se deberá indicar, en forma expresa y destacada, la posibilidad del titular de los datos de ejercer sus derechos de oposición y supresión.

3. Los datos referentes a la salud sólo podrán 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 podrán 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 de los artículos 15 y 22 inciso 1 de la presente ley y la mención de su derecho a oponerse al tratamiento de sus datos.

4. En los supuestos contemplados en el presente artículo, el titular de los datos podrá ejercer el derecho de acceso sin cargo ni limitación temporal alguna. La información a suministrarle deberá 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.

5. El titular cuyos datos sean objeto de tratamiento a que se refiere el presente artículo podrá ejercer en cualquier momento los derechos de oposición y supresión regulados por los artículos 30 y 31 de la presente ley, sin perjuicio de lo establecido por el Capítulo V.

Capítulo VII

Autoridad de control

ARTÍCULO 61. - (Autoridad de control).

1. Créase la Agencia Nacional de Protección de Datos Personales (ANPDP) como órgano de control que debe velar por el cumplimiento de los principios y procedimientos establecidos en la presente ley.

2. La ANPDP gozará de autonomía funcional y actuará como órgano descentralizado en el ámbito del Ministerio de Justicia y Derechos Humanos de la Nación.

3. La ANPDP será dirigida y administrada por un Director designado por el término de cuatro (4) años, por el Poder Ejecutivo con acuerdo del Senado de la Nación, debiendo ser seleccionado entre personas con antecedentes en la materia. El director a cargo de la ANPDP tendrá rango y jerarquía de secretario.

4. El Director tendrá dedicación exclusiva en su función, encontrándose alcanzado por las incompatibilidades fijadas por ley para los funcionarios públicos y cesará de pleno derecho en sus funciones de mediar alguna de las siguientes circunstancias:

a) Renuncia;

b) Vencimiento del mandato;

c) Fallecimiento; y

d) Estar comprendido en alguna situación que le genere incompatibilidad o inhabilidad.

5. El Director podrá ser removido por mal desempeño, por delito en el ejercicio de sus funciones o por crímenes comunes. El Poder Ejecutivo nacional llevará adelante el procedimiento de remoción del director de la ANPDP, dándole intervención a una comisión bicameral del Honorable Congreso de la Nación, que será presidida por el presidente del Senado y estará integrada por los presidentes de las comisiones de Asuntos Constitucionales y de Derechos y Garantías de la Honorable Cámara de Senadores de la Nación y las de Asuntos Constitucionales y de Derechos Humanos y Garantías de la Honorable Cámara de Diputados de la Nación, quien emitirá un dictamen vinculante.

6. La ANPDP contará con el personal técnico y administrativo que establezca la ley de presupuesto general de la administración nacional. El personal estará obligado a guardar secreto respecto de los datos de carácter personal de los que tome conocimiento en el desarrollo de sus funciones.

7. LA ANPDP se financiará a través de:

a) Lo que recaude en concepto de tasas por los servicios que preste;

b) El producido de las multas referidas en esta ley;

c) Las asignaciones presupuestarias que se incluyan en la Ley de Presupuesto de la Administración Nacional.

ARTÍCULO 62. - (Facultades de la autoridad de control).

La ANPDP deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la presente ley. A tales efectos tendrá las siguientes funciones y atribuciones:

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

b) Dictar las normas y reglamentaciones 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 reglamentaciones 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 la presente ley;

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 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) Diseñar su estructura orgánica de funcionamiento y designar a su planta de agentes;

k) Elaborar su presupuesto anual;

l) Solicitar información a los delegados de protección de datos en los términos de lo previsto la presente ley;

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

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

o) 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 VIII

Procedimientos y Sanciones

ARTÍCULO 63. - (Procedimiento).

1. A los efectos de constatar el cumplimiento de las disposiciones de la presente ley, la autoridad de control podrá iniciar:

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

b) Procedimientos de verificación de oficio;

c) Procedimientos de verificación por denuncia de un tercero.

2. La autoridad de control podrá en cualquier momento del procedimiento buscar una conciliación entre el titular de los datos y el responsable del tratamiento.

3. De llegarse a un acuerdo de conciliación entre ambos, esté se hará constar por escrito y tendrá efectos vinculantes.

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

ARTÍCULO 64. - (Trámite de protección de los datos personales).

1. El titular de los datos o su representante legal, podrá 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 y expresando con claridad el contenido de su requerimiento y de los preceptos de esta ley que se consideran vulnerados. La presentación deberá 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 inciso 2 de la presente ley.

2. En el caso de que el titular de los datos no reciba respuesta por parte del responsable del tratamiento bastará que el titular de los datos acredite la fecha en que presentó la solicitud ante el responsable del tratamiento.

3. Iniciado el trámite de protección de los datos personales previsto en este artículo ante la autoridad de control, se dará traslado del mismo al responsable del tratamiento, para que, en el plazo de cinco (5) días, 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 estime 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 tres (3) días siguientes a su notificación.

ARTÍCULO 65. - (Trámite de verificación de oficio o por denuncia de un tercero).

1. La autoridad de control verificará el cumplimiento de la presente ley y de la normatividad que de esta derive. La verificación podrá iniciarse de oficio o por denuncia de un tercero.

2. A efectos de practicar la verificación prevista en el inciso anterior, 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.

3. En caso de que corresponda, se aplicará al trámite lo previsto en el artículo 64 inciso 3 de la presente ley.

ARTÍCULO 66. - (Resolución).

1. La resolución de la autoridad de control podrá:

a) Archivar los trámites mencionados en los artículos 64 y 65 de la presente ley.

b) En caso de considerar que asiste derecho al titular de los datos, requerirle al responsable del tratamiento para 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 de efectuado.

c) Imponer una sanción en caso que se hubieran verificado incumplimientos a la presente ley.

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

ARTÍCULO 67. - (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. No

procederá el recurso de alzada. Agotada la vía administrativa, las resoluciones que impongan sanciones serán recurribles por ante la Cámara Nacional de Apelaciones en lo Contencioso Administrativo Federal de la Capital Federal.

ARTÍCULO 68. - (Sanciones).

1. La autoridad de control, una vez establecido el incumplimiento de las disposiciones de la presente ley por parte del responsable del tratamiento o del encargado del tratamiento, adoptará las medidas o impondrá las sanciones correspondientes.

2. La autoridad de control podrá imponer a los responsables del tratamiento y encargados del tratamiento las siguientes sanciones:

a) Apercibimientos;

b) Multas que podrán alcanzar el equivalente a quinientos (500) Salarios Mínimo Vital y Móvil vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó;

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;

3. Al ordenar la suspensión o cierres previstos en los apartados 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 y/o direccionen, almacenen, alojen, intermedien, enlacen y/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 donde se encuentren alojados los datos personales o los procedimientos para acceder al mismo.

4. Las sanciones indicadas en el presente artículo sólo 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.

5. Las sanciones por infracciones a las que se refieren el inciso 2, 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;

g) 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 IX

Acción de Habeas Data

ARTÍCULO 69. - (Procedencia).

1. La acción de habeas data procederá:

a) Para ejercer el derecho de acceso previsto en el artículo 27 de la presente ley.

b) 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 habeas 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.

c) Para ejercer el derecho a la portabilidad de los datos personales previsto en el artículo 33 cuando los datos personales se encuentren en bases de datos públicas o privadas.

ARTÍCULO 70 - (Legitimación activa y pasiva).

1. La acción de habeas data podrá ser ejercida por el titular de los datos afectado, 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 físicas fallecidas, la acción podrá ser ejercida por sus sucesores universales.

2. En el proceso podrá intervenir en forma coadyuvante y cuando corresponda la autoridad de control prevista en esta ley, quien será notificada del inicio de la acción de habeas data.

3. La acción procederá respecto de los responsables del tratamiento, con las excepciones previstas en los artículos 3 y 36 de la presente ley.

ARTÍCULO 71. - (Competencia).

1. Será competente para entender en esta acción el juez del domicilio del actor, o del demandado a elección del actor.

2. 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 72. - (Procedimiento aplicable).

1. La acción de habeas data tramitará según las disposiciones de la presente ley y por el procedimiento que corresponde a la acción de amparo común y supletoriamente por las normas del Código Procesal Civil y Comercial de la Nación, en lo atinente al juicio sumarísimo.

ARTÍCULO 73. - (Requisitos de la demanda).

1. La demanda deberá interponerse por escrito, individualizando con la mayor precisión posible el nombre y domicilio del responsable de la base de datos, 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 dependen el responsable o el encargado.

2. El accionante deberá alegar las razones por las cuales entiende que en la base de datos obra información referida a su persona; los motivos por los cuales considera que procede el ejercicio de los derechos que le reconoce la presente ley. Deberá asimismo justificar que se han cumplido los recaudos que hacen al ejercicio de tales derechos.

3. El titular del dato podrá solicitar que mientras dure el procedimiento el responsable o el encargado del tratamiento informe cuando corresponda que la información cuestionada está sometida a un proceso judicial.

4. El juez podrá disponer el bloqueo provisional del acceso a la base de datos en lo referente al dato personal motivo del juicio cuando sea manifiesto el carácter ilícito del tratamiento de esos datos o ellos sean inequívocamente falsos o inexactos.

ARTÍCULO 74. - (Trámite).

1. Admitida la acción el juez requerirá al responsable del tratamiento la remisión de la información concerniente al accionante. 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.

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

3. 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.

4. 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 75. - (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 incluyó la información cuestionada y aquellas por las que no evacuó el pedido efectuado por el titular de los datos.

ARTÍCULO 76. - (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 el término de tres (3) días.

ARTÍCULO 77. - (Sentencia).

1. Vencido el plazo para la contestación del informe o contestado el mismo, y en el supuesto del artículo anterior, luego de contestada la ampliación, y habiendo sido producida en su caso la prueba, el juez dictará sentencia.

2. En el caso de estimarse procedente la acción, se especificará si la información debe ser bloqueada, suprimida, rectificada, actualizada o declarada confidencial, estableciendo un plazo para su cumplimiento.

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

4. En cualquier caso, la sentencia deberá ser comunicada al organismo de control.

Capítulo X

Disposiciones transitorias

ARTÍCULO 78. – (Estructura de la Autoridad de Control).

En el plazo de sesenta (60) días hábiles posteriores a la asunción de su cargo, el Director de la ANPDP presentará un proyecto de estructura organizativa y reglamentación interna, para su aprobación por el Poder Ejecutivo Nacional y publicación en el Boletín Oficial.

ARTÍCULO 79. – (Presupuesto).

1. Autorízase al Poder Ejecutivo Nacional a realizar las modificaciones e incorporaciones en la ley de presupuesto de gastos y recursos de la administración nacional para el ejercicio fiscal vigente en los aspectos que se consideren necesarios para la implementación de la presente ley.

2. Deberá preverse en el presupuesto del año inmediato subsiguiente la incorporación de los recursos necesarios para el correcto cumplimiento de las funciones de la ANPDP.

ARTÍCULO 80. – (Reglamentación).

1. El Poder Ejecutivo nacional reglamentará la presente ley dentro de los ciento ochenta (180) días desde su promulgación.

ARTÍCULO 81. – (Vigencia).

1. Las disposiciones de la presente ley entrarán en vigencia al año de su publicación en el Boletín Oficial.

2. Los responsables y encargados del tratamiento de datos contarán con el plazo máximo de un (1) año 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 la ley Nº 25.326, Nº 26.951, sus normas reglamentarias y demás disposiciones de la Dirección Nacional de Protección de Datos Personales.

3. El Registro Nacional “No Llame” creado por la ley Nº 26.951 será transferido al nuevo Registro creado en el artículo Nº 46 de la presente ley de acuerdo a lo que prevea su reglamentación.

Capítulo XI

Disposiciones finales

ARTÍCULO 82. - (Orden público y jurisdicción federal).

1. Las normas de la presente ley contenidas en los Capítulos I a VI son de orden público y de aplicación en lo pertinente en todo el territorio nacional.

2. Se invita a las provincias a adherir a las normas de esta ley que fueren de aplicación exclusiva en jurisdicción nacional.

3. 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. - (Derogación).

1. Deróganse las leyes Nº 25.326 y Nº 26.951.

ARTÍCULO 84. - Comuníquese al Poder Ejecutivo Nacional.