</'Guía de Buenas Prácticas para el desarrollo de Apps'>

< Resumen de la Disposición DNPDP N°18/15 para proteger de forma adecuada los datos personales en tus Apps / >;

PDP
Dirección Nacional de Protección de Datos Personales

Ministerio de Justicia y Derechos Humanos
Presidencia de la Nación

////////////////////// < Colaboró: fundación SADOSKY Investigación y Desarrollo en TIC
Presidencia de la Nación
Ministerio de Ciencia, Tecnología e Innovación Productiva >

< Índice>

< Introducción >

Las aplicaciones, como programas de software, tienen la capacidad de recabar, usar y transferir información de carácter personal. Esta información se encuentra protegida por la Ley N° 25.326 (Ley de Protección de Datos Personales - LPDP), que establece ciertos principios y obligaciones que tiene que cumplir cualquier tratamiento de datos. Esta Ley define al dato personal como cualquier información que pueda referirse a una persona determinada o determinable, así que desde el nombre y apellido hasta una imagen o una grabación de voz, cuando permita reconocer a una persona, es un dato protegido.

El principio más importante que establece la Ley es que el dato, sin importar dónde se encuentre almacenado o cómo se esté utilizando, es siempre de propiedad de su titular, quien tiene el derecho a controlar los usos que se le dan a su información personal.

Como desarrollador de aplicaciones, tenés la responsabilidad de velar por la privacidad de los datos personales que tus software utilicen. Debés tener en cuenta cómo tus programas protegerán la privacidad desde el inicio mismo del desarrollo, teniendo una política de uso de los datos clara, transparente, que les permita a los titulares de datos conocer cómo es el tratamiento de datos que tus programas realizan.

La Dirección Nacional de Protección de Datos Personales (PDP) es la Autoridad de Aplicación de la LPDP y, desde nuestras funciones de control de cumplimiento de la Ley, estimulamos una cultura de protección de los datos personales. Mediante esta Guía te brindamos las herramientas necesarias para que puedas contemplar la protección de datos personales en tus desarrollos de software. De esta manera, al mismo tiempo, vas a cumplir con la Ley y a generar en tus clientes, usuarios y titulares de los datos, la confianza en que tus productos respetan la privacidad.

Cabe señalar que, en 2003, la Unión Europea (UE) otorgó a la normativa argentina la adecuación en los términos establecidos por la Directiva N° 95/46/CE, razón por la cual a nuestro país no se le aplican restricciones para la transferencia de datos personales desde la UE. Por lo tanto, al cumplir con la legislación argentina, también vas a cumplir con los estándares normativos europeos.

< Principios de privacidad >

CONSENTIMIENTO DEL TITULAR DE LOS DATOS

El consentimiento del titular para el uso de su información personal es la única manera en la que el tratamiento de datos es lícito, salvo que se trate de alguna excepción prevista por la Ley. El consentimiento implica una decisión informada por parte del titular permitiendo el uso de sus datos. Recabá el consentimiento de los titulares y, al mismo tiempo, informales que estarás recabando su información y los usos que le darás.

FINALIDAD

Los datos que tus aplicaciones recolecten solo pueden ser utilizados conforme con la finalidad que originó la recolección. Si la aplicación que desarrollás está destinada a la gestión contable de un comercio, por ejemplo la información personal que se recabe puede utilizarse para llevar la contabilidad, liquidar impuestos, llevar inventarios y todas las finalidades compatibles a una gestión contable, pero no podría utilizarse para llevar adelante una campaña publicitaria, porque se estaría cambiando la finalidad del tratamiento.

CALIDAD DE LOS DATOS

Los datos personales que tus aplicaciones recaben y almacenen deben ser ciertos, adecuados, pertinentes y no excesivos en relación con la finalidad que motivó su recolección. No pueden ser obtenidos por medios desleales o fraudulentos y deben ser destruidos cuando hayan dejado de ser útiles. Además, tenés la obligación de almacenarlos de manera tal que se facilite el ejercicio de los derechos de sus titulares.

SEGURIDAD

La seguridad de la información es un aspecto importante de la protección de datos. Evaluá los riesgos de seguridad que tu aplicación puede aparejar, teniendo en cuenta la sensibilidad de la información personal que recolecta y almacena. Verificá que tu aplicación, si utiliza datos personales, respete las mejores prácticas en seguridad de la información.

CONFIDENCIALIDAD

Los datos personales de los que tomes conocimiento debido al tratamiento que realices son confidenciales. Está prohibido revelarlos. Esta obligación alcanza a cualquier persona que intervenga en cualquier etapa del desarrollo, e inclusive subsiste aun finalizada la relación contractual.

LOS 8 PASOS BÁSICOS PARA DESARROLLAR RESGUARDANDO LA PRIVACIDAD

1. CONTEMPLÁ LA PRIVACIDAD EN TODOS LOS PROCESOS DE TU ORGANIZACIÓN.

2. DESARROLLÁ LAS APLICACIONES CON EL CONCEPTO DE "PRIVACIDAD DESDE EL DISEÑO".

3. ESTABLECÉ UNA POLÍTICA DE PRIVACIDAD CLARA Y FÁCILMENTE ACCESIBLE POR LOS TITULARES DEL DATO.

4. CONFIGURÁ POR DEFECTO COMO "ACTIVADAS" LAS OPCIONES DE PRIVACIDAD.

5. PERMITÍ A LOS TITULARES DEL DATO QUE ELIJAN Y CONTROLEN LA CONFIGURACIÓN DE PRIVACIDAD.

6. LIMITÁ LA CANTIDAD DE DATOS QUE RECOLECTÁS O RETENÉS. NO RECOLECTES O ALMACENES INFORMACIÓN PERSONAL QUE TU SISTEMA, APLICACIÓN O DISPOSITIVO NO NECESITE. EVITÁ RECOLECTAR O ALMACENAR DATOS SENSIBLES, SALVO QUE ESTÉS AUTORIZADO A HACERLO. ESTABLECÉ UNA POLÍTICA PARA LA ELIMINACIÓN DE DATOS PERSONALES QUE YA NO TE SEAN ÚTILES.

7. ASEGURÁ LOS DATOS PERSONALES RECABADOS.

8. ASUMÍ LA RESPONSABILIDAD: DESIGNÁ A UN "RESPONSABLE DE PRIVACIDAD" O ASUMÍ VOS MISMO LA RESPONSABILIDAD DEL RESGUARDO DE LOS DATOS PERSONALES QUE HAYAS TRATADO.

3 METODOLOGÍAS PARA TENER EN CUENTA:

PRIVACY BY DESIGN

"Privacidad desde el diseño" es un enfoque en el que se contempla la protección de la privacidad desde el origen mismo del diseño de un sistema, aplicación o dispositivo. Desde esta perspectiva, la preocupación por la protección de los datos personales no debe ser analizada posteriormente a la finalización del desarrollo, como si se tratara de un anexo, sino que debe estar presente en todas las etapas del proceso. De este modo, la privacidad se considera en todas las fases del ciclo de vida del sistema, aplicación o dispositivo.

PRIVACY BY DEFAULT

Es un concepto de desarrollo de software que establece que la configuración de la privacidad debe estar "activada" de manera predeterminada, de manera tal que implique un acto de voluntad del titular desactivar o compartir información personal. Generalmente los titulares del dato, cuando hacen uso de aplicaciones, no saben cómo configurar la privacidad o no se toman el tiempo para hacerlo. Por ello, es importante que la aplicación no comparta información personal, a menos que el titular configure las opciones de privacidad permitiéndolo.

PRIVACY-ENHANCING TECHNOLOGIES (PET)

Se trata de un sistema de medidas, herramientas y aplicaciones que protegen la privacidad de la información mediante la eliminación o minimización de los datos personales. De ese modo, se previene el procesamiento innecesario o indeseado de datos personales, sin la pérdida de la funcionalidad del sistema de información.

i. *Herramientas de gestión de la privacidad, que permitan al titular elegir y controlar la forma en que sus datos son recolectados y usados.*

ii. *Herramientas de protección de la privacidad*

1. *Disociación de datos*
Herramientas que apuntan a ocultar la identidad del titular, para que no puedan relacionarse los datos con una persona determinada o determinable. Por ejemplo, las herramientas que ocultan la dirección IP del emisor.

2. *Seudonimización*
Permiten llevar adelante operaciones sin que se determine al titular del dato, identificado solo con un seudónimo.

3. *Seguridad de la información*
El objetivo principal es impedir el acceso no autorizado a los sistemas, archivos o a las comunicaciones a través de una red.

4. *Metadatos*

Se utilizan para incorporar etiquetas a los archivos que contengan datos personales, agregándoles información que detalle la fuente, el consentimiento obtenido, cómo puede ser utilizado, así como las políticas de privacidad a las que está sujeto. Además, puede incorporarse información que indique la cantidad de tiempo que los datos personales se pueden conservar o si el titular brindó consentimiento para ceder la información a terceros.

5. *Criptografía*

Utilizada no solo para almacenar información de manera segura, sino también para asegurar su integridad al transportarla, ya sea mediante soportes físicos como a través de una red, o para generar accesos seguros a datos personales.

ASPECTOS TÉCNICOS PARA APLICACIONES

i. *Correcta utilización de los permisos*

Si se trata de una aplicación móvil, verificá que los permisos que requiere sean los estrictamente necesarios para el funcionamiento adecuado. Las personas guardan en sus dispositivos móviles información muy personal, y una mala administración de los permisos los dejará vulnerables. Un ejemplo típico del mal uso de los permisos es una aplicación de linterna que requiera acceso a los contactos del titular del dato o a su calendario.

ii. *Geolocalización*

Si tu aplicación accede a datos de localización, debés notificar y obtener el permiso del titular del dato, incluso si se trata de metadatos de geolocalización de fotos o videos.

< Establecimiento de una política de privacidad >

Uno de los pasos más importantes para respetar la privacidad de los titulares de datos es desarrollar una Política de Privacidad que explique claramente qué tipo de información se recaba, cómo se usa y con quién la compartís. Esta política debe ser simple y, en la medida de lo posible, estandarizada, de manera tal que se facilite su lectura y comprensión por parte de los titulares de datos. Es importante que la política refleje el tratamiento de datos que hace tu aplicación, así que no “cortes y pegues” una política genérica de otra aplicación o desarrollador. Por el contrario, desarrollá una que sea comprensiva de las particularidades de tu aplicación. Tené en cuenta que una Política de Privacidad que no responda al tratamiento de datos que hagas puede generarte inconvenientes con tus clientes, los titulares de datos de la aplicación y hasta los organismos de control, como esta PDP.

a. Un aspecto que no debés olvidar es que, si introducís cambios en la Política de Privacidad, deberás notificarlas. La Política de Privacidad debe cumplir con los siguientes lineamientos:

1. Contener una definición del Objeto de la Política de Privacidad (cuál es el objeto tutelado, como, por ejemplo los artículos 1° y 2° de la LPDP y sus principios), alcance (a quiénes resulta exigible la política) y su compatibilidad y/o relación con las políticas de protección de la información comercial o cualquier otra política que entre en conjunción con la protección de datos personales.

2. Incluir una definición de los términos utilizados en la política (acordes con la LPDP).

3. Reflejar los principios de protección de datos personales aplicables al tratamiento de datos que haga la aplicación (acordes con la LPDP, según artículos 3°, 4°, 5°, 6°, 7°).

4. Si compartís o transferís los datos con un tercero, debés notificarlo en forma destacada en tu política y cumplir con los requisitos de la cesión de datos, contemplados en el artículo 11 de la LPDP.

5. Contemplá la confidencialidad de los datos personales (artículo 10, LPDP), con referencia a los convenios de confidencialidad del personal y terceros que presten servicios, y de cualquier otra persona u organización que puedan entrar en conocimiento de los datos personales que trata la aplicación.

6. Hacer mención a la política de seguridad de los datos personales, y a la aplicación de la Disposición DNPDP N° 11/06 (manual de seguridad).

7. Contemplá, en el caso de que el tratamiento de datos incluya su transferencia al exterior, los requisitos para una Transferencia Internacional de datos personales (aplicando el artículo 12 LPDP y Decreto N° 1558/01). **Tené en cuenta que el almacenamiento en la nube se considera una transferencia internacional de datos.**

8. En el caso de que el uso de la información personal incluya la finalidad de publicidad, debe contemplarse el cumplimiento de las obligaciones específicas para este tipo de tratamiento (artículo 27 LPDP y Decreto N° 1558/01, Disposiciones DNPDP N° 10/08 y 4/09).

9. Tené en cuenta lo que establece el artículo 25 LPDP y Decreto N° 1558/01 en relación con las prestaciones de servicios de tratamiento de datos por cuenta de terceros.

10. Establecé el procedimiento para cumplir con los derechos de los titulares de los datos (derechos de acceso, rectificación, supresión y bloqueo, artículos 14, 15, 16 y 27, inc. 3 de la LPDP).

11. Comunicá, mediante la Política, quién es el Encargado de Protección de Datos (a cargo de velar por la correcta y efectiva aplicación de la política y su relación, tanto con los titulares de datos, como con el órgano de control). Puede ser una persona física o un área dentro de tu organización.

b. Asegurate de que alguien en tu organización sea responsable de la privacidad. Al menos una persona en la organización debe velar por que las aplicaciones que desarrolles cumplan con los principios de la protección de datos. Si se trata de un emprendimiento unipersonal, debés encargarte vos mismo de esta función.

Será tarea de esta persona:

- Asegurarse de que las aplicaciones y el tratamiento de datos que hagan cumplan con la normativa de protección de datos (Ley N° 25.326, decreto reglamentario, disposición de la DNPDP).
- Revisar y mantener actualizada la Política de Privacidad de la organización, y asegurarse de que las aplicaciones que desarrollan la cumplen.
- Responder las consultas vinculadas con la Política de Privacidad, el ejercicio de los derechos del titular del dato y los requerimientos de la PDP.

c. Capacitación del personal en privacidad. Todas las personas que trabajen en tu organización deben estar al tanto de las obligaciones que tienen con relación al tratamiento de datos. Es la mejor manera de evitar que, por error o desconocimiento, hagan incurrir a tu organización en un incumplimiento.

d. Control de terceros con los que se intercambian datos personales. La Ley N° 25.326 establece la responsabilidad solidaria entre quienes intercambian información. Es decir, que si a quien le mandás o de quien recibís información personal comete algún incumplimiento, también te podrían reclamar a vos. Solamente cedé o recibí datos personales de personas u organizaciones confiables, y verificá que se encuentren debidamente inscriptos en el Registro Nacional de Bases de Datos de la PDP.

< Control de la información personal por parte de sus titulares >

Brindales a quienes hagan uso de tus aplicaciones, y a los titulares de los datos en general, el control de su información personal, particularmente cuando se trata de información sensible, íntima o cuando se le den usos que no sean los obvios o comunes. Los usos que se hagan de los datos personales deben provenir de una elección consciente e informada de sus titulares.

Permitiles acceder a la información que almacenes sobre ellos y dáles la posibilidad de rectificar información errónea o desactualizada, o de suprimirla, cuando corresponda. Además, debés esforzarte para que la información personal que almacenás sea cierta, adecuada, pertinente y no excesiva con relación a los usos que le das y que motivaron su recolección.

Procurá recabar, siempre que sea necesario, el consentimiento del titular del dato para usar su información personal. Tratá de limitar al mínimo posible, y a lo estrictamente necesario, la cantidad de información personal que recolectás y utilizás, y destruí de manera segura aquellos datos que te hayan dejado de ser útiles.

< Aplicaciones móviles >

Las aplicaciones desarrolladas para dispositivos móviles generalmente tendrán la limitación del tamaño de la pantalla. Deberás ser creativo para poder mostrar la información de tu Política de Privacidad de una manera que les resulte útil a los titulares de datos, con el desafío adicional que genera un espacio pequeño como la pantalla de un teléfono celular.

Algunos consejos que podés aplicar:

_

a. *Separar la información en distintas capas*

Pocas personas estarán dispuestas a leer 30 páginas de una Política de Privacidad, y mucho menos en la pequeña pantalla de un celular. Para evitarlo, deberás clasificar la información que brindás en tu Política de Privacidad, separarla en distintas capas y colocar la más importante en las capas superiores. Luego, ofrecer hipervínculos para aquellos que quieran profundizar más y conocer los detalles.

_

b. *Proveer al titular del dato un tablero de privacidad*

Podría ser útil ofrecer una herramienta de configuración de privacidad, con un diseño atractivo y amigable, que le permita al titular del dato elegir fácilmente las opciones de privacidad.

_

c. *Utilizar técnicas para llamar la atención del titular del dato*

Debés procurar llamar la atención del titular del dato sobre la información importante de tu Política de Privacidad.

Para ello, podés recurrir a una serie de recursos que te brinda la plataforma móvil, como indicaciones visuales o sonoras:

_

Gráficos: Utilizá íconos, etiquetas o imágenes que llamen la atención del titular del dato, vinculados a un texto que provea más información. Esto puede resultar útil en determinado momento del uso de la aplicación, como cuando se disponga a utilizar los datos personales del titular del dato. Por ejemplo, si se va a geolocalizar una foto, se activa un símbolo que advierte de esto al titular del dato y, de ser necesario, se recaba su consentimiento.

_

Colores: Llamá la atención de los titulares de datos mediante el uso de colores y la variación de su intensidad. Esta puede ser proporcional a la importancia de la decisión o sensibilidad de la información.

_

Sonidos: Otro modo apropiado de llamar la atención del titular del dato es a través de sonidos. Por ejemplo, cuando sea necesaria una decisión del titular del dato o debas proveerlo de información importante acerca del uso de sus datos personales.

< Uso de aplicaciones por niñ@s >

Si tu aplicación puede ser usada por niñ@s o adolescentes, deberás procurar un cuidado especial. Se trata de un grupo que hace un uso intensivo de la tecnología, que la sabe manejar, pero que, por su edad, puede carecer de la reflexión crítica necesaria para identificar los peligros que el mal uso de su información personal puede aparejar.
Son una población vulnerable y, por lo tanto, será necesario tener en cuenta recaudos especiales para resguardarlos.

- Limitá al máximo el tipo y la cantidad de información que recolectás sobre ellos.
- Contemplá estrictas medidas de seguridad sobre la información que necesariamente debas recabar.
- Evitá compartir información personal de menores con terceros.
- Brindales información adecuada a su nivel de comprensión sobre el uso responsable de sus datos y alertalos sobre los peligros que se relacionan con una mala utilización.
- Siempre que corresponda, obtené el consentimiento de sus padres. Establecé mecanismos de resguardo para mantenerlos informados acerca de los usos que se hacen de la información personal de los menores.

<Contacto con la PDP y legislación aplicable >

PDP
Dirección Nacional de Protección de Datos Personales

La **PDP** es un órgano dependiente del **MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS**, con sede en Sarmiento 1118, piso 5°, de la CIUDAD AUTÓNOMA DE BUENOS AIRES.

En su página web *(www.jus.gov.ar/datospersonales)* podrás encontrar toda la normativa de protección de datos personales, que incluye la LPDP, su decreto reglamentario y todas las disposiciones del Director Nacional de Protección de Datos Personales, así como otra información adicional sobre privacidad y protección de datos.

< SABÍAS QUE la PDP también cuenta con: >

El REGISTRO NACIONAL DE BASES DE DATOS, donde los titulares o usuarios de bases de datos tienen la obligación de registrarse. Es un requisito que establece la Ley N° 25.326 para que las bases sean consideradas lícitas y para facilitar el derecho de acceso, rectificación, actualización o supresión por parte de los titulares de los datos.

REGISTRO NACIONAL
NO LLAME
LA DECISIÓN ES TUYA

El REGISTRO NACIONAL NO LLAME, a fin de limitar las llamadas y los mensajes de publicidad que recibís en tu teléfono. La inscripción es gratuita y muy sencilla: llamá al 146 desde el número que querés dar de alta, o ingresá tu solicitud en ***www.nollame.gob.ar.***

CENTRO DE ASISTENCIA
A LAS VÍCTIMAS DE
ROBO DE IDENTIDAD

El CENTRO DE ASISTENCIA A LAS VÍCTIMAS DE ROBO DE IDENTIDAD y el REGISTRO NACIONAL DE DOCUMENTOS DE IDENTIDAD CUESTIONADOS, en donde podés consultar los documentos de identidad denunciados por las autoridades públicas competentes y/o sus titulares, con motivo de pérdida, hurto, robo o cualquier otra alteración.

CENTRO de CAPACITACIÓN, INVESTIGACIÓN y DIFUSIÓN de la PROTECCIÓN de los DATOS PERSONALES

El CENTRO DE CAPACITACIÓN, INVESTIGACIÓN Y DIFUSIÓN DE LA PROTECCIÓN DE LOS DATOS PERSONALES, donde funciona el **Campus Virtual PDP,** en el que podés realizar varios cursos virtuales referentes a esta temática, desde cualquier punto del país.

con vos en la web

El Programa Nacional CON VOS EN LA WEB, que ayuda a niñas, niños y adolescentes a desarrollar las capacidades críticas y reflexivas para un uso responsable de las nuevas tecnologías. También genera contenidos y capacitaciones para padres y docentes, con el fin de acompañar a chicas y chicos a cuidar su intimidad y privacidad en las redes sociales e Internet.

PROTECCION DE LOS DATOS PERSONALES
Ley 25.326

Disposiciones Generales. Principios generales relativos a la protección de datos. Derechos de los titulares de datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones. Acción de protección de los datos personales.

Sancionada: Octubre 4 de 2000.

Promulgada Parcialmente: Octubre 30 de 2000.

El Senado y Cámara de Diputados de la Nación Argentina reunidos en Congreso, etc. sancionan con fuerza de Ley:

Ley de Protección de los Datos Personales

CAPÍTULO I

DISPOSICIONES GENERALES

ARTICULO 1° — (Objeto).

La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional.

Las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal.
En ningún caso se podrán afectar la base de datos ni las fuentes de información periodísticas.

ARTICULO 2° — (Definiciones).

A los fines de la presente ley se entiende por:

— Datos personales: Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.

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

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

— Tratamiento de datos: Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación,

relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

— Responsable de archivo, registro, base o banco de datos: Persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos.

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

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

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

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

Capítulo II

Principios generales relativos a la protección de datos

ARTICULO 3° — (Archivos de datos – Licitud).

La formación de archivos de datos será lícita cuando se encuentren debidamente inscriptos, observando en su operación los principios que establece la presente ley y las reglamentaciones que se dicten en su consecuencia.

Los archivos de datos no pueden tener finalidades contrarias a las leyes o a la moral pública.

ARTICULO 4° — (Calidad de los datos).

1. Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido.

2. La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley.

3. Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.

4. Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario.

5. Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados, por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular establecidos en el artículo 16 de la presente ley.

6. Los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular.

7. Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados.

ARTICULO 5° — (Consentimiento).

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

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

2. No será necesario el consentimiento cuando:

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

b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal;

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

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

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

ARTICULO 6° — (Información).

Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara:

a) La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios;

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

c) El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos referidos en el artículo siguiente;

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

e) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos.

ARTICULO 7° — (Categoría de datos).

1. Ninguna persona puede ser obligada a proporcionar datos sensibles.

2. Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares.

3. Queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles. Sin perjuicio de ello, la Iglesia Católica, las asociaciones religiosas y las organizaciones políticas y sindicales podrán llevar un registro de sus miembros.

4. Los datos relativos a antecedentes penales o contravencionales sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas.

ARTICULO 8° — (Datos relativos a la salud).

Los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando los principios del secreto profesional.

ARTICULO 9° — (Seguridad de los datos).

1. El responsable o usuario del archivo de datos debe 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. Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.

ARTICULO 10. — (Deber de confidencialidad).

1. El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aun después de finalizada su relación con el titular del archivo de datos.

2. El obligado podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública.

ARTICULO 11. — (Cesión).

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

2. El consentimiento para la cesión es revocable.

3. El consentimiento no es exigido cuando:

a) Así lo disponga una ley;

b) En los supuestos previstos en el artículo 5° inciso 2;

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

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

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

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

ARTICULO 12. — (Transferencia internacional).

1. Es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no propocionen niveles de protección adecuados.

2. La prohibición 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 tanto se realice en los términos del inciso e) del artículo anterior;

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

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

e) Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico.

Capítulo III

Derechos de los titulares de datos

ARTICULO 13. — (Derecho de Información).

Toda persona puede solicitar información al organismo de control relativa a la existencia de archivos, registros, bases o bancos de datos personales, sus finalidades y la identidad de sus responsables.

El registro que se lleve al efecto será de consulta pública y gratuita.

ARTICULO 14. — (Derecho de acceso).

1. El titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes.

2. El responsable o usuario debe proporcionar la información solicitada dentro de los diez días corridos de haber sido intimado fehacientemente.
Vencido el plazo sin que se satisfaga el pedido, o si evacuado el informe, éste se estimara insuficiente, quedará expedita la acción de protección de los datos personales o de hábeas data prevista en esta ley.

3. El derecho de acceso a que se refiere este artículo sólo puede ser ejercido en forma gratuita a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al efecto.

4. El ejercicio del derecho al cual se refiere este artículo en el caso de datos de personas fallecidas le corresponderá a sus sucesores universales.

ARTICULO 15. — (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.

2. La información debe ser amplia y versar sobre la totalidad del registro perteneciente al titular, 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 interesado.

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

ARTICULO 16. — (Derecho de rectificación, actualización o supresión).

1. Toda persona tiene derecho a que sean rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad los datos personales de los que sea titular, que estén incluidos en un banco de datos.

2. El responsable o usuario del banco de datos, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias a tal fin en el plazo máximo de cinco días hábiles de recibido el reclamo del titular de los datos o advertido el error o falsedad.

3. El incumplimiento de esta obligación dentro del término acordado en el inciso precedente, habilitará al interesado a promover sin más la acción de protección de los datos personales o de hábeas data prevista en la presente ley.

4. En el supuesto de cesión, o transferencia de datos, el responsable o usuario del banco de datos debe notificar la rectificación o supresión al cesionario dentro del quinto día hábil de efectuado el tratamiento del dato.

5. La supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos.

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

7. Los datos personales deben ser conservados durante los plazos previstos en las disposiciones aplicables o en su caso, en las contractuales entre el responsable o usuario del banco de datos y el titular de los datos.

ARTICULO 17. — (Excepciones).

1. Los responsables o usuarios de bancos de datos públicos pueden, mediante decisión fundada, denegar el acceso, rectificación 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 o usuarios de bancos de datos públicos, 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. Sin perjuicio de lo establecido en los incisos anteriores, se deberá brindar acceso a los registros en cuestión en la oportunidad en que el afectado tenga que ejercer su derecho de defensa.

ARTICULO 18. — (Comisiones legislativas).

Las Comisiones de Defensa Nacional y la Comisión Bicameral de Fiscalización de los Organos y Actividades de Seguridad Interior e Inteligencia del Congreso de la Nación y la Comisión de Seguridad Interior de la Cámara de Diputados de la Nación, o las que las sustituyan, tendrán acceso a los archivos o bancos de datos referidos en el artículo 23 inciso 2 por razones fundadas y en aquellos aspectos que constituyan materia de competencia de tales Comisiones.

ARTICULO 19. — (Gratuidad).
La rectificación, actualización o supresión de datos personales inexactos o incompletos que obren en registros públicos o privados se efectuará sin cargo alguno para el interesado.

ARTICULO 20. — (Impugnación de valoraciones personales).

1. Las decisiones judiciales o los actos administrativos que impliquen apreciación o valoración de conductas humanas, no podrán tener como único fundamento el resultado del tratamiento informatizado de datos personales que suministren una definición del perfil o personalidad del interesado.

2. Los actos que resulten contrarios a la disposición precedente serán insanablemente nulos.

Capítulo IV

Usuarios y responsables de archivos, registros y bancos de datos

ARTICULO 21. — (Registro de archivos de datos. Inscripción).

1. Todo archivo, registro, base o banco de datos público, y privado destinado a proporcionar informes debe inscribirse en el Registro que al efecto habilite el organismo de control.

2. El registro de archivos de datos debe comprender como mínimo la siguiente información:

a) Nombre y domicilio del responsable;

b) Características y finalidad del archivo;

c) Naturaleza de los datos personales contenidos en cada archivo;

d) Forma de recolección y actualización de datos;

e) Destino de los datos y personas físicas o de existencia ideal a las que pueden ser transmitidos;

f) Modo de interrelacionar la información registrada;

g) Medios utilizados para garantizar la seguridad de los datos, debiendo detallar la categoría de personas con acceso al tratamiento de la información;

h) Tiempo de conservación de los datos;

i) Forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para la rectificación o actualización de los datos.

3) Ningún usuario de datos podrá poseer datos personales de naturaleza distinta a los declarados en el registro.

El incumplimiento de estos requisitos dará lugar a las sanciones administrativas previstas en el capítulo VI de la presente ley.

ARTICULO 22. — (Archivos, registros o bancos de datos públicos).

1. Las normas sobre creación, modificación o supresión de archivos, registros o bancos de datos pertenecientes a organismos públicos deben hacerse por medio de disposición general publicada en el Boletín Oficial de la Nación o diario oficial.

2. Las disposiciones respectivas, deben indicar:

a) Características y finalidad del archivo;

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

c) Procedimiento de obtención y actualización de los datos;

d) Estructura básica del archivo, informatizado o no, y la descripción de la naturaleza de los datos personales que contendrán;

e) Las cesiones, transferencias o interconexiones previstas;

f) Organos responsables del archivo, precisando dependencia jerárquica en su caso;

g) Las oficinas ante las que se pudiesen efectuar las reclamaciones en ejercicio de los derechos de acceso, rectificación o supresión.

3. En las disposiciones que se dicten para la supresión de los registros informatizados se esta blecerá el destino de los mismos o las medidas que se adopten para su destrucción.

ARTICULO 23. — (Supuestos especiales).

1. Quedarán sujetos al régimen de la presente ley, los datos personales que por haberse almacenado para fines administrativos, deban ser objeto de registro permanente en los bancos de datos de las fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia; y aquellos sobre antecedentes personales que proporcionen dichos bancos de datos a las autoridades administrativas o judiciales que los requieran en virtud de disposiciones legales.

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, sin consentimiento de los afectados, queda limitado a aquellos supuestos y categoría 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. Los archivos, en tales casos, deberán ser específicos y establecidos al efecto, debiendo clasificarse por categorías, en función de su grado de fiabilidad.

3. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

ARTICULO 24. — (Archivos, registros o bancos de datos privados).

Los particulares que formen archivos, registros o bancos de datos que no sean para un uso exclusivamente personal deberán registrarse conforme lo previsto en el artículo 21.

ARTICULO 25. — (Prestación de servicios informatizados de datos personales).

1. Cuando por cuenta de terceros se presten servicios de tratamiento de datos personales, éstos no podrán aplicarse o utilizarse con un fin distinto al que figure en el contrato de

servicios, ni cederlos a otras personas, ni aun para su conservación.

2. Una vez cumplida la prestación contractual los datos personales tratados deberán ser destruidos, salvo que medie autorización expresa de aquel por cuenta de quien se prestan tales servicios cuando razonablemente se presuma la posibilidad de ulteriores encargos, en cuyo caso se podrá almacenar con las debidas condiciones de seguridad por un período de hasta dos años.

ARTICULO 26. — (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 usuario del banco de datos, le comunicará las informaciones, evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y 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 años. Dicho plazo se reducirá a dos años cuando el deudor cancele o de otro modo extinga la obligación, debiéndose hace constar dicho hecho.

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.

ARTICULO 27. — (Archivos, registros o bancos de datos con fines de publicidad).

1. En la recopilación de domicilios, reparto de documentos, publicidad o venta directa y otras actividades análogas, se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo, cuando éstos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento.

2. En los supuestos contemplados en el presente artículo, el titular de los datos podrá ejercer el derecho de acceso sin cargo alguno.

3. El titular podrá en cualquier momento solicitar el retiro o bloqueo de su nombre de los bancos de datos a los que se refiere el presente artículo.

ARTICULO 28. — (Archivos, registros o bancos de datos relativos a encuestas).

1. Las normas de la presente ley no se aplicarán a las encuestas de opinión, mediciones y estadísticas relevadas conforme a Ley 17.622, trabajos de prospección de mercados,

investigaciones científicas o médicas y actividades análogas, en la medida que los datos recogidos no puedan atribuirse a una persona determinada o determinable.

2. Si en el proceso de recolección de datos no resultara posible mantener el anonimato, se deberá utilizar una técnica de disociación, de modo que no permita identificar a persona alguna.

Capítulo V

Control

ARTICULO 29. — (Organo de Control).

1. El órgano de control 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;

c) Realizar un censo de archivos, registros o bancos de datos alcanzados por la ley y mantener el registro permanente de los mismos;

d) Controlar la observancia de las normas sobre integridad y seguridad de datos por parte de los archivos, registros o bancos de datos. 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 los datos personales 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) Constituirse en querellante en las acciones penales que se promovieran por violaciones a la presente ley;

h) Controlar el cumplimiento de los requisitos y garantías que deben reunir los archivos o bancos de datos privados destinados a suministrar informes, para obtener la correspondiente inscripción en el Registro creado por esta ley.

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

3. El órgano de control será dirigido y administrado 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 tendrá dedicación exclusiva en su función, encontrándose alcanzado por las incompatibilidades fijadas por ley para los funcionarios públicos y podrá ser removido por el Poder Ejecutivo por mal desempeño de sus funciones.

ARTICULO 30. — (Códigos de conducta).

1. Las asociaciones o entidades representativas de responsables o usuarios de bancos de datos de titularidad privada podrán elaborar códigos de conducta de práctica profesional, que establezcan normas para el tratamiento de datos personales que tiendan a asegurar y mejorar las condiciones de operación de los sistemas de información en función de los principios establecidos en la presente ley.

2. Dichos códigos deberán ser inscriptos en el registro que al efecto lleve el organismo de control, quien podrá denegar la inscripción cuando considere que no se ajustan a las disposiciones legales y reglamentarias sobre la materia.

Capítulo VI

Sanciones

ARTICULO 31. — (Sanciones administrativas).

1. Sin perjuicio de las responsabilidades administrativas que correspondan en los casos de responsables o usuarios de bancos de datos públicos; de la responsabilidad por daños y perjuicios derivados de la inobservancia de la presente ley, y de las sanciones penales que correspondan, el organismo de control podrá aplicar las sanciones de apercibimiento, suspensión, multa de mil pesos ($ 1.000.-) a cien mil pesos ($ 100.000.-), clausura o cancelación del archivo, registro o banco de datos.

2. La reglamentación determinará las condiciones y procedimientos para la aplicación de las sanciones previstas, las que deberán graduarse en relación a la gravedad y extensión de la violación y de los perjuicios derivados de la infracción, garantizando el principio del debido proceso.

ARTICULO 32. — (Sanciones penales).

1. Incorpórase como artículo 117 bis del Código Penal, el siguiente:
"1°. Será reprimido con la pena de prisión de un mes a dos años el que insertara o hiciera insertar a sabiendas datos falsos en un archivo de datos personales.

2°. La pena será de seis meses a tres años, al que proporcionara a un tercero a sabiendas información falsa contenida en un archivo de datos personales.

3°. La escala penal se aumentará en la mitad del mínimo y del máximo, cuando del hecho se derive perjuicio a alguna persona.

4°. Cuando el autor o responsable del ilícito sea funcionario público en ejercicio de sus funciones, se le aplicará la accesoria de inhabilitación para el desempeño de cargos públicos por el doble del tiempo que el de la condena".

2. Incorpórase como artículo 157 bis del Código Penal el siguiente:

"Será reprimido con la pena de prisión de un mes a dos años el que:
1°. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;

2°. Revelare a otro información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley.
Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años".

Capítulo VII

Acción de protección de los datos personales

ARTICULO 33. — (Procedencia).

1. La acción de protección de los datos personales o de hábeas data procederá:
a) para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquéllos;

b) en los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido en la presente ley, para exigir su rectificación, supresión, confidencialidad o actualización.
ARTICULO 34. — (Legitimación activa).

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

Cuando la acción sea ejercida por personas de existencia ideal, deberá ser interpuesta por sus representantes legales, o apoderados que éstas designen al efecto.
En el proceso podrá intervenir en forma coadyuvante el Defensor del Pueblo.

ARTICULO 35. — (Legitimación pasiva).

La acción procederá respecto de los responsables y usuarios de bancos de datos públicos, y de los privados destinados a proveer informes.

ARTICULO 36. — (Competencia).

Será competente para entender en esta acción el juez del domicilio del actor; el del domicilio del demandado; el del lugar en el que el hecho o acto se exteriorice o pudiera tener efecto, a elección del actor.

Procederá la competencia federal:

a) cuando se interponga en contra de archivos de datos públicos de organismos nacionales, y
b) cuando los archivos de datos se encuentren interconectados en redes interjurisdicciones, nacionales o internacionales.

ARTICULO 37. — (Procedimiento aplicable).

La acción de hábeas 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.

ARTICULO 38. — (Requisitos de la demanda).

1. La demanda deberá interponerse por escrito, individualizando con la mayor precisión posible el nombre y domicilio del archivo, registro o banco de datos y, en su caso, el nombre del responsable o usuario del mismo.

En el caso de los archivos, registros o bancos públicos, se procurará establecer el organismo estatal del cual dependen.

2. El accionante deberá alegar las razones por las cuales entiende que en el archivo, registro o banco de datos individualizado obra información referida a su persona; los motivos por los cuales considera que la información que le atañe resulta discriminatoria, falsa o inexacta y justificar que se han cumplido los recaudos que hacen al ejercicio de los derechos que le reconoce la presente ley.

3. El afectado podrá solicitar que mientras dure el procedimiento, el registro o banco de datos asiente que la información cuestionada está sometida a un proceso judicial.

4. El Juez podrá disponer el bloqueo provisional del archivo en lo referente al dato personal motivo del juicio cuando sea manifiesto el carácter discriminatorio, falso o inexacto de la información de que se trate.

5. A los efectos de requerir información al archivo, registro o banco de datos involucrado, el criterio judicial de apreciación de las circunstancias requeridas en los puntos 1 y 2 debe ser amplio.

ARTICULO 39. — (Trámite).

1. Admitida la acción el juez requerirá al archivo, registro o banco de datos la remisión de la información concerniente al accionante. Podrá asimismo solicitar 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 días hábiles, el que podrá ser ampliado prudencialmente por el juez.

ARTICULO 40. — (Confidencialidad de la información).

1. Los registros, archivos o bancos de datos privados no podrán alegar la confidencialidad de la información que se les requiere salvo el caso en que se afecten las fuentes de información periodística.

2. Cuando un archivo, registro o banco de datos público se oponga a la remisión del informe solicitado con invocación de las excepciones al derecho de acceso, rectificación o supresión, 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 los datos solicitados asegurando el mantenimiento de su confidencialidad.

ARTICULO 41. — (Contestación del informe).

Al contestar el informe, el archivo, registro o banco 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 interesado, de conformidad a lo establecido en los artículos 13 a 15 de la ley.

ARTICULO 42. — (Ampliación de la demanda).

Contestado el informe, el actor podrá, en el término de tres días, ampliar el objeto de la demanda solicitando la supresión, rectificación, confidencialidad o actualización de sus datos personales, en los casos que resulte procedente a tenor de la presente ley, ofreciendo en el mismo acto la prueba pertinente. De esta presentación se dará traslado al demandado por el término de tres días.

ARTICULO 43. — (Sentencia).

1. Vencido el plazo para la contestación del informe o contestado el mismo, y en el supuesto del artículo 42, 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 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, que deberá llevar un registro al efecto.

ARTICULO 44. — (Ambito de aplicación).

Las normas de la presente ley contenidas en los Capítulos I, II, III y IV, y artículo 32 son de orden público y de aplicación en lo pertinente en todo el territorio nacional.
Se invita a las provincias a adherir a las normas de esta ley que fueren de aplicación exclusiva en jurisdicción nacional.

La jurisdicción federal regirá respecto de los registros, archivos, bases o bancos de datos interconectados en redes de alcance interjurisdiccional, nacional o internacional.

ARTICULO 45. — El Poder Ejecutivo Nacional deberá reglamentar la presente ley y establecer el organismo de control dentro de los ciento ochenta días de su promulgación.

ARTICULO 46. — (Disposiciones transitorias).

Los archivos, registros, bases o bancos de datos destinados a proporcionar informes, existentes al momento de la sanción de la presente ley, deberán inscribirse en el registro que se habilite conforme a lo dispuesto en el artículo 21 y adecuarse a lo que dispone el presente

régimen dentro del plazo que al efecto establezca la reglamentación.

ARTICULO 47. — Los bancos de datos prestadores de servicios de información crediticia deberán suprimir, o en su caso, omitir asentar, todo dato referido al incumplimiento o mora en el pago de una obligación, si ésta hubiere sido cancelada al momento de la entrada en vigencia de la presente ley.

ARTICULO 48. — Comuníquese al Poder Ejecutivo.

DADA EN LA SALA DE SESIONES DEL CONGRESO ARGENTINO, EN BUENOS AIRES, A LOS CUATRO DIAS DEL MES DE OCTUBRE DEL AÑO DOS MIL.

— REGISTRADO BAJO EL N° 25.326 —

Sarmiento 1118 - 5º Piso - Ciudad Autónoma de Buenos Aires - C1041AAX
infodnpdp@jus.gob.ar - **Teléfono:** (+5411) 5300-4000 - Interno 76701
Denuncias: (+5411) 5300-4089 - **Registro:** (+5411) 5300-4088
www.jus.gob.ar/datospersonales

PDP

Dirección Nacional de Protección
de Datos Personales

Ministerio de
Justicia y Derechos Humanos
Presidencia de la Nación