

# SESIONES ORDINARIAS

## 2000

### ORDEN DEL DIA Nº 776

#### COMISIONES DE ASUNTOS CONSTITUCIONALES, DE JUSTICIA, DE LEGISLACION GENERAL, DE LEGISLACION PENAL Y DE PRESUPUESTO Y HACIENDA

Impreso el día 4 de septiembre de 2000

Término del artículo 113: 13 de septiembre de 2000

SUMARIO: Ley sobre protección de los datos personales y reglamentación del artículo 43 de la Constitución Nacional. (230-S-1998 )

#### Dictamen de las comisiones

##### *Honorable Cámara:*

Las comisiones de Asuntos Constitucionales; de Justicia, de Legislación General, de Legislación Penal y de Presupuesto y Hacienda han considerado el proyecto de ley venido en revisión del Honorable Senado sobre protección de los datos personales y reglamentación del artículo 43 de la Constitución Nacional y han tenido a la vista los de los señores diputados Maqueda, Godoy, Natale, Menem y Quintela, Carrió y otros, y, por las razones expuestas en el informe que se acompaña, y las que dará el miembro informante aconsejan la sanción del siguiente

#### PROYECTO DE LEY

*El Senado y Cámara de Diputados, ...*

#### CAPÍTULO I

##### *Disposiciones generales*

Artículo 1º — *Objeto.* La presente ley tiene por objeto regular.

- a) El uso y tratamiento de datos personales contenidos en archivos, registros, o cualquier otro medio técnico de tratamiento de datos públicos, o privados destinados a dar informes, con el fin de garantizar el pleno ejercicio de los derechos de sus titulares, y

- b) La tutela jurisdiccional de estos derechos, de conformidad con 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

Art 2º — *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 o política 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 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.
- *Medios o redes de difusión pública o semi-pública de alcance nacional e internacional.* Toda utilización de la red Internet, así como sus variaciones intranet y extranet. Intranet es toda red que utilizando o aprovechando las tecnologías de Internet se utiliza dentro del ámbito privado. Extranet combina ambos tipos de redes extendiendo su alcance desde el ámbito privado al global siendo soportado por la plataforma existente de Internet.

## CAPÍTULO II

*Principios generales relativos a la protección de datos*

Art. 3° — *Archivo 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.

Art. 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 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.

Art. 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 datos que tengan fines estadísticos a los que se les hubiera aplicado una operación de disociación;
- f) Se trate de información proveniente de operaciones comerciales o financieras que realicen los socios de asociaciones empresarias de informaciones comerciales, sin fines de lucro, con la condición de que esa información se utilice exclusivamente entre los socios de tales asociaciones.

Art. 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.

Art. 7° — *Categoría de datos*.

1. Con la salvedad que se establece en el inciso siguiente, queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles así como también el tratamiento de dichos datos y de cualquiera otro que revele ideología, raza, religión, hábitos personales y comportamiento sexual.

No se considerarían comprendidos, a los fines de la presente ley, en la expresión "hábitos personales" los que se refieran a hábitos de consumo de bienes y servicios,

siempre que dichos hábitos no revelen directamente o indirectamente, los comprendidos en la definición de 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. 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.

Art. 8° — *Datos relativos a la salud*. Los hospitales y demás instituciones sanitarias públicas o privadas, y los profesionales vinculados a la ciencia médica 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.

Art. 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.

Art. 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 aún 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.

Art. 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 cesio

nario 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. Será nulo el consentimiento cuando no recaiga sobre un cesionario determinado o determinable, o si no constase con claridad la finalidad de la cesión que se consiente.

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 5º apartado 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 indistinguibles.

#### Art. 12. — *Transferencia internacional.*

1. Es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección semejantes a los que establece la presente ley. En ningún caso podrán ser objeto de transferencia internacional los datos sensibles
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;
- f) Cuando la transferencia se realice dentro del mismo conjunto económico, entre controlante y controlada o entre sociedades que tengan un controlante común;
- g) Cuando el cedente obligue contractualmente al cesionario y se responsabilice frente al titular de los datos, previamente a la transferencia, a cumplir con las normas de la presente ley.

### CAPÍTULO III

#### *Derechos de los titulares de datos*

Art. 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.

#### Art. 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 expedida la acción de conocimiento en los términos previstos en el capítulo VII sección I de la presente 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.

#### Art. 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.

**Art. 16. — Derecho de rectificación, actualización o supresión.**

1. Toda persona tiene derecho a que sean rectificadas, 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 de un 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 haber 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 reparación en los términos previstos en el capítulo VII, sección 1, de 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.

**Art. 17. — Excepciones.**

1. Los responsables de bancos de datos públicos pueden, mediante decisión fundada, denegar el acceso, rectificación o la supresión de datos de carácter personal en función de

la protección de la defensa de la Nación, 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.

**Art. 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 22, inciso 2, por razones fundadas y en aquellos aspectos que constituyan materia de competencia de tales comisiones.

**Art. 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.

**Art. 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*

**Art. 21. — Registros 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.

**Art. 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 y supresión.

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

**Art. 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 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. Los archivos, en tales casos, deberán ser específicos y establecidos al efecto, debiendo clasificarse por categoría, 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.

**Art. 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.

**Art. 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 ex-

presa de aquel por cuenta de quien se prestan tales servicios cuando razonablemente se presume la posibilidad de ulteriores encargos, en cuyo caso se podrá almacenar con las debidas condiciones de seguridad por un período de hasta dos años.

**Art. 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. Los datos relacionados con el incumplimiento de obligaciones dinerarias sólo podrán tratarse si concurren los siguientes recaudos:

- a) Existencia previa de una deuda cierta, vencida y exigible, que haya resultado impaga;
- b) Requerimiento previo de pago a su deudor o a quien corresponda el cumplimiento de la obligación.

3. A solicitud del titular de los datos, al 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 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 tres años cuando el deudor cancele o de otro modo extinga la obligación, debiéndose hacer 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, pero sí la ulterior comunicación de ésta si se verificaren incumplimientos de conformidad con lo establecido en el inciso 2, cuando estén relacionados con el giro de las actividades comerciales o crediticias de los cesionarios.

**Art. 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.

**Art. 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, 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

**Art. 29. — Órgano 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 autarquía funcional y actuará como órgano descentralizado en el ámbito del Ministerio de Justicia 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 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, incapacidad sobreviviente o condena por delito doloso.

El director, así como también el resto del personal, están obligados a guardar secreto de los datos de carácter personal que conozcan en el desarrollo de su función.

La Fiscalía de Investigaciones Administrativas, a través de un fiscal general competente en la materia, podrá ejercer las facultades previstas en el artículo 45 de la ley 24.946 respecto de la observancia de la presente por parte de todos los archivos, registros y

bases de datos públicos. Dictaminará en los asuntos de importancia sometidos a consideración del director; en los casos en que se haya denegado el acceso o rectificación de datos invocando las causales del artículo 17 incisos 1 y 2 su intervención será obligatoria.

#### Art. 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*

#### Art. 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.

#### Art. 32. — *Sanciones penales.*

1. Incorporase como artículo 117 bis del Código Penal, el siguiente:

- 1º Será reprimido con la pena de prisión de un mes a dos años el que insertare o hiciere insertar a sabiendas datos falsos en un archivo de datos personales.



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

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

4º Cuando el autor o responsable del ilícito sea funcionario público en ejercicio de sus funciones, se aplicará la accesoria de inhabilitación para el desempeño de cargos públicos por el doble 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:

1º A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos accediere, de cualquier forma, a un banco de datos personales

2º Revelare a otro información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley.

Quando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años.

## CAPÍTULO VII

### De la tutela judicial

#### Sección 1

##### *Acciones especiales de hábeas data*

Art. 33. — *Objeto.* Las normas contenidas en el presente capítulo tienen por finalidad otorgar a la persona legitimada el acceso a una vía procesal sumarisima y expedita que le permita obtener del órgano judicial competente, en forma inmediata, la protección o, en su caso, el restablecimiento del pleno ejercicio de los derechos a que se refiere la presente ley, haciendo cesar cualquier tipo de amenaza, intromisión o violación de los mismos.

Art. 34. — *Acción de conocimiento.* Toda persona de existencia visible o ideal podrá demandar judicialmente una orden para conocer la amplitud, tenor, destino o uso de los datos referidos a ella acumulados en cualquier tipo de registros o bancos de datos de entidades públicas o privadas, incluidos los destinados a proveer informes y los sistemas informáticos.

Art. 35. — *Acción de prevención.* Toda persona de existencia visible o ideal tendrá acción para demandar judicialmente la adopción de todas las medidas que resulten necesarias para impedir que se concrete

cualquier clase de violación, restricción, limitación o intromisión ilegítima de sus derechos, en el tratamiento de sus datos personales.

Art. 36. — *Acción de reparación.* Toda persona de existencia visible o ideal tendrá acción para demandar judicialmente la supresión, rectificación, actualización o confidencialidad de sus datos personales, en caso de error, falsedad, obsolescencia o discriminación, y el restablecimiento en el goce de los derechos reconocidos por esta ley. Las medidas a adoptar podrán incluir las que resulten necesarias para prevenir o impedir violaciones, restricciones o intromisiones ulteriores.

Art. 37. — *Acumulación de acciones.* Las acciones descritas en los artículos anteriores, podrán ser interpuestas en forma autónoma, o ser susceptibles de acumulación.

#### Sección 2

##### *De las acciones de hábeas data en general*

Art. 38. — *Legitimación activa.* Las acciones previstas en la sección 1 del presente capítulo, podrán ser ejercidas por el afectado, sus tutores o curadores y los sucesores de las personas físicas, sean en líneas directa o colateral hasta el segundo grado, por sí o por intermedio de apoderado.

Quando la acción sea ejercida por personas de existencia ideal, deberá ser interpuesta por sus representantes legales, o apoderados que éstas designen al efecto.

Art. 39. — *Legitimación pasiva.* La acción procederá respecto de los responsables y usuarios de bancos de datos públicos, y de los privados destinados a proveer informes.

Art. 40. — *Competencia.* Será competente para entender en las acciones previstas en la sección 1 de este capítulo, el Tribunal Civil del domicilio del actor, del demandado o el del lugar de la amenaza, violación o intromisión ilegítima, a elección del actor.

Art. 41. — *Procedimiento.* En todos los casos de ejercicio de alguna de las acciones indicadas en el artículo precedente el procedimiento a aplicar será el de mayor celeridad previsto en la jurisdicción competente. La ausencia en la jurisdicción correspondiente, de una vía procesal específica y apta para el ejercicio de dichas acciones no será obstáculo para la actuación del Tribunal, que deberá aplicar el procedimiento previsto que más se adecue al caso planteado, con las adaptaciones que resulten necesarias a fin de lograr la finalidad tutelar eficaz y oportuna.

En el ámbito de la jurisdicción nacional, las acciones mencionadas se tramitarán, por el procedimiento sumarisimo establecido en el Código Procesal Civil y Comercial de la Nación.

Art. 42. — *Requisitos de procedencia.* Para la procedencia de las acciones previstas en el presente capítulo, el actor sólo deberá acreditar sumariamente:

- a) En el supuesto de la acción de prevención, la existencia de amenaza a alguno de los derechos reconocidos por esta ley,
- b) En los supuestos de las acciones de cono-  
cimiento y reparación, el cumplimiento de los recaudos previstos en el inciso 2 del artículo 14, y en el inciso 3 del artículo 16, respectivamente.

En ningún caso será necesaria la atribución de culpa o dolo. Son innecesarios la protesta o reclamo administrativo previo, o su agotamiento, cuando la acción judicial se plantee contra una persona jurídica pública.

Art. 43. — *Medidas cautelares.* Durante la sustanciación de las acciones previstas en el presente capítulo, el tribunal, de oficio o a petición de parte, deberá dictar las medidas cautelares, provisionales o de urgencia que resulten necesarias para hacer cesar de inmediato la amenaza, violación o intromisión ilegítima de los derechos previstos en el presente régimen. El tribunal podrá requerir del actor el cumplimiento de la contracautela pertinente, sólo en el supuesto que por su naturaleza, las medidas a adoptar sean susceptibles de causar perjuicio a la parte demandada.

Art. 44. — *Sentencia.* La sentencia que haga lugar a la acción ordenará la adopción de las medidas necesarias para asegurar la protección o el restablecimiento del derecho afectado, debiendo en su caso, disponer la rectificación, actualización o eliminación de los datos de carácter personal, sin perjuicio de la indemnización que pudiera corresponder. En caso de deducirse recurso de apelación éste tendrá sólo carácter devolutivo.

Art. 45. — *Compatibilidad con otros procesos.* El ejercicio de las acciones de protección y defensa previstas en este capítulo no obstará al trámite de naturaleza penal que pudiera corresponder, ni el reclamo por los daños y perjuicios causados que se ejercerá según lo dispuesto en las normas pertinentes. La existencia de causa penal no será obstáculo para el dictado de sentencia en las acciones previstas por esta ley.

Art. 46. — *Presunción.* En los supuestos en que se demande judicialmente el resarcimiento de los daños ocasionados, la existencia de perjuicio se presumirá siempre que se acredite la violación o intromisión ilegítima en los derechos reconocidos por esta ley. La indemnización se extenderá al daño moral que se valorará atendiendo a las circunstancias del caso y a la gravedad de la lesión efectivamente producida. La condena podrá incluir la difusión y/o publicación de la sentencia por los medios que resulten

necesarios para la adecuada compensación del perjuicio causado. La indemnización nunca será inferior a \$ 5.000.

Art. 47. — *Ámbito de aplicación.* Las normas de la presente ley contenidas en los capítulos I, II, III, IV y VII, y artículo 32 son de orden público y de aplicación en todo el territorio nacional.

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

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

Art. 48. — El Poder Ejecutivo deberá reglamentar la presente ley y establecer el organismo de control dentro de los ciento ochenta días de su promulgación.

Art. 49. — *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 lo dispuesto en el artículo 21 y adecuarse a lo que dispone el presente régimen dentro del plazo que al efecto establezca la reglamentación.

Art. 50. — Comuníquese al Poder Ejecutivo.

Sala de las comisiones, 28 de agosto de 2000.

Elisa M. Carrió. — René H. Balestra. — José G. Dumón. — Dámaso Larraburu. — Carlos E. Soria. — Guillermo H. De Sanctis. — Bernardo P. Quinzio. — Julio A. Tejerina. — Ramón H. Torres Molina. — Atilio P. Tazzioli. — Enrique G. Cardesa. — Nilda C. Garré. — José A. Vitar. — Ricardo Gómez Díez. — Simón F. Hernández. — Miguel A. Giubergia. — Miguel A. Abe-  
lla. — Guillermo E. Corfield. — Gustavo C. Galland. — Darío P. Alessandro. — Juan C. Ayala. — Manuel J. Baladrón. — Carlos M. Balter. — Fortunato R. Cambareri. — María L. Chaya. — María T. Colombo. — Melchor R. Cruchaga. — Roberto R. de Barriazarra. — José M. Díaz Bancalari. — Alejandro N. Fernández. — Cristina E. Fernández de Kirchner. — Pablo A. Fontdevila. — Graciela M. Giannettasio. — Rubén H. Giustiniani. — Cristina R. Guevara. — Guillermo R. Jenejes. — Adrián Menem. — Horacio F. Pernasetti. — Héctor T. Polino. — José A. Recio. — Rodolfo Rodil. — Jesús Rodríguez. — Pedro Salvatori. — Liliana F. Sánchez. — Eduardo Santín. — Juan M. Urtubey. — Silvia B. Vázquez. — Jorge Zapata Mercader.

En disidencia:

*Eduardo R. Di Cola.*

En disidencia parcial:

*Raúl E. Baglini. — Jorge A. Baldrich. —  
Jorge P. Busti. — Graciela Camaño. —  
Alfredo J. Castañón. — Franco A. Ca-  
vaglia. — Guillermo A. Francos. —  
Teodoro R. Funes. — Arturo R. Lafalla  
Jorge R. Matzkin. — Ana M. Mosso  
— Carlos D. Snopek.*

## INFORME

*Honorable Cámara:*

Habiendo estudiado en profundidad el tema en cuestión las comisiones de Asuntos Constitucionales. de Justicia; de Legislación General; de Legislación Penal y de Presupuesto y Hacienda entienden que debe aprobarse el texto que se acompaña, en materia de protección de datos personales, reglamentando el artículo 43 de la Constitución Nacional por las razones que oportunamente se brindaran.

*Elisa M. Carrió.*

## FUNDAMENTOS DE LA DISIDENCIA PARCIAL DEL SEÑOR DIPUTADO RAUL BAGLINI

Señor presidente:

Fundamento la disidencia planteada en la necesidad de distinguir con claridad el tratamiento que se debe dar a los datos provenientes de concurso o quiebras, cuya conservación en los bancos de datos por un plazo más extenso de tiempo es de interés legítimo para la actividad crediticia, de la del simple deudor que cancela o extingue la obligación adeudada. Los plazos propuestos, para uno u otro caso, son sustancialmente distintos en cuanto a su extensión, fundados —precisamente— en la diferente significación que reviste su conservación en orden a evaluar el riesgo crediticio.

En la misma línea que lo anterior, la información sobre obligaciones dinerarias cuyo origen no sea crediticio, deberá ser eliminada de los archivos no bien se produzca su cancelación. Tal temperamento obedece a que, una vez cancelada, pierden su relevancia a los fines de la actividad crediticia.

Particular importancia reviste la obligación que las entidades crediticias tienen de notificar —en el plazo fijado por la ley— a los bancos de datos públicos o privados de la cancelación o extinción de deudas por parte del deudor. Tal obligación tiende a asegurar el cumplimiento de derechos de raigambre constitucional. Otro tanto puede decirse de la notificación fehaciente que se deberá hacer al deudor acerca del cumplimiento de esta obligación.

La modificación que se propone al artículo 26 inciso 5 tiende a precisar el sentido de lo en él dispuesto.

Respecto del artículo 29 inciso 1 del dictamen se precisa que el órgano de control actuará en el ámbito del Ministerio de Justicia de la Nación como como órgano descentralizado, por ello, se proponen las siguientes modificaciones:

## Artículo 26.

Inciso 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 tres años cuando el deudor cancele o de otro modo extinga la obligación. En el caso de datos originados en concursos o quiebras, este plazo se extenderá a diez años. Tratándose de obligaciones dinerarias de origen no crediticio, su cancelación u otro modo de extinción implicará que dicha información, una vez producidas las notificaciones que se establecen en este inciso, debe ser eliminada de los archivos que se ceden. Está a cargo de la entidad crediticia la obligación de notificar a los bancos de datos públicos o privados la cancelación o la extinción de la deuda por parte del deudor, dentro de las cuarenta y ocho horas de producida. Asimismo, deberá notificar fehacientemente al deudor acerca del cumplimiento de esta obligación.

Inciso 5 La prestación de servicios de información crediticia no requerirá el previo consentimiento del titular de los datos a los efectos de su cesión, pero si la ulterior comunicación al acreedor si se verificaren incumplimientos de conformidad con lo establecido en el inciso 2, cuando estén relacionados con el giro de las actividades comerciales o crediticias de los cesionarios.

## Artículo 29.

Inciso 1: El órgano de control actuará como órgano descentralizado en el ámbito del Ministerio de Justicia de la Nación.

Inciso 2 Corresponde al inciso 1 del dictamen.

*Raúl E. Baglini.*

## FUNDAMENTOS DE LA DISIDENCIA PARCIAL DE LA SEÑORA DIPUTADA CAMAÑO

Señor presidente:

Tengo el agrado de dirigirme a usted en mi condición de diputada, integrante de la Comisión de Presupuesto y Hacienda de la Honorable Cámara bajo su digno cargo, a los fines de hacer llegar las razones sobre cuyas bases doy sustento y fundamentación a mi disidencia parcial con relación al proyecto de ley que hace al expediente de la referencia.

En tal sentido señalo de mi parte la necesidad de que el proyecto en cuestión deje expresamente establecido que en modo alguno la ley reglamentaria del artículo 43, párrafo tercero de la Cons-

titución Nacional (hábeas data) importa la derogación de norma alguna contenida en la Ley Orgánica del Instituto Nacional de Estadística y Censos (INDEC), 17.622.

Así lo solicito en función de que por ésta se ampara el secreto estadístico, determinando en tal sentido su artículo 10 que las informaciones que se suministran a los organismos que integran el Sistema Estadístico Nacional son estrictamente secretas y sólo utilizables con fines estadísticos.

La observancia de dicho principio es la que posibilita alcanzar o mantener niveles óptimos de excelencia en lo concerniente a relevamiento, captura, procesamiento y ulterior difusión de datos.

Corresponde a tal efecto destacar cómo todo el proceso relativo a la elaboración de las estadísticas y de la información que se obtiene por medio de los operativos censales, se basa y sustenta en la confiabilidad que el sistema ofrece a los informantes desde que asegura la preservación de la confidencialidad de la información y su utilización circunscripta a un único fin: el estadístico.

Además la protección de la intimidad personal se compadece en este caso con la postura propiciada.

Metodológicamente, la inserción bien podría realizarse como último párrafo en el artículo 1º; o bien como último punto (3) del artículo 10; último punto (4) del artículo 22; punto 3 del artículo 28 o como artículo 50, previo al de forma.

Sin otro particular que esperar sean atendidas las razones expuestas fundantes de mi disidencia parcial, hago propicia la ocasión para saludarlo en mi consideración más distinguida.

*Graciela Camaño.*

#### FUNDAMENTOS DE LA DISIDENCIA PARCIAL DEL SEÑOR DIPUTADO FRANCO CAVIGLIA

Señor presidente:

La acción de amparo especial de hábeas data fue incorporada a nuestro ordenamiento constitucional en la reforma de la Carta Magna de 1994, en el artículo 43 tercer párrafo, delegándose en el Congreso Nacional su reglamentación.

El Senado de la Nación en noviembre de 1998 dio media sanción a un proyecto de ley y desde el año pasado los senadores demandan para que Diputados finalice su labor, al punto que recientemente la Comisión de Asuntos Constitucionales del Honorable Senado de la Nación, con fecha 2 de junio de 2000, aprobó un dictamen dirigido a la Cámara de Diputados en términos muy duros, los que no comparto y rechazo abiertamente, y por el cual se nos hace responsables de que este proyecto de hábeas data duerma el sueño de los justos, cosa que no ha sido así.

No obstante comparto con los señores senadores que es imperioso sancionar esta ley, ya que de lo

contrario se producirá la caducidad de proyecto en noviembre de 2000, y con ello se generará una imagen altamente negativa para la Cámara. Existe en la opinión pública una convicción generalizada que las extraordinarias transformaciones que experimenta la sociedad día a día al influjo del progreso tecnológico, de la informática y las telecomunicaciones, amenazan gravemente su privacidad.

Las disidencias que a continuación expondré, tienen relación con el grave problema de la inseguridad que sufre nuestra sociedad y abarcan un aspecto público y otro privado, bajo el común denominador del delito no convencional.

Señor presidente, esta posición no es nueva y tiene su directa relación con mi proyecto de código de delitos no convencionales (6.702-D.-99). El crimen organizado ha incorporado a su accionar las nuevas tecnologías, contando con equipos de avanzada para el desarrollo de actividades ilícitas, a la vez que la criminalidad ha derivado en el establecimiento de alianzas internacionales, entre las distintas organizaciones.

#### *Seguridad pública*

La primera observación se centra en el artículo 23 inciso 3 ("Supuestos especiales") que trata de los datos personales que son objeto de registro permanente en los bancos de datos de las fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia.

El Estado tiene como misión primordial proveer a la seguridad. Es una condición *sine qua non* que las fuerzas de seguridad dominen el uso de las nuevas tecnologías para instrumentar políticas de prevención en especial en la lucha contra el contrabando, narcotráfico y terrorismo, entre otros graves delitos no convencionales que asuelan nuestra sociedad y para ello es vital realizar cruzamientos de datos.

A esta lucha se le suma que el rasgo más importante de la globalización es la interconexión de los mercados productivos y financieros y la transnacionalización empresarial. En sí mismo, esto no es ni bueno ni malo, si no es que esta nueva estructura global es aprovechada para la comisión de un abanico de delitos en donde las organizaciones criminales corrompen funcionarios públicos y cometen fraude económico además de las actividades criminales tradicionales. Con el avance de las comunicaciones y en especial la aparición de Internet y el comercio electrónico, las transacciones de dinero asistémico se han tornado de una complejidad difícil de detectar. Una operación de lavado puede nacer en Colombia, ingresar a través de diversas operaciones a los Estados Unidos y terminar como dinero legal en Suiza, donde luego será utilizado para inversiones, por ejemplo, en el área de construcciones en Brasil.

El crimen no convencional adquirió un estado multidimensional, a diferencia del pasado donde las principales organizaciones criminales se dedicaban exclusivamente al tráfico de drogas, la trata de blan-

cas y el control del juego clandestino. Hoy interactúan en verdaderas redes globales y descentralizadas. Es decir, diversificación (1), transnacionalización (2) e interacción (3).

El avance tecnológico que se ha dado en los últimos años en el campo de la informática, las telecomunicaciones y el transporte ha contribuido a que el crimen organizado esté en mejor posición para ocultar sus actividades y utilizar más fácilmente cuantiosos recursos que obtiene de ellas.

La única forma de contrarrestar este fenómeno es la utilización de nuevos instrumentos de investigación para ponernos a la altura de los acontecimientos, siendo la información un recurso estratégico en la formulación de políticas nacionales y regionales.

El concepto de investigación científica por parte de los Estados, a nivel interno y externo, fue reformulado en función de establecer interrelaciones entre las figuras investigativas, la investigación estadística y el estudio académico de los diferentes conflictos. Es innegable que los delitos provenientes del narcotráfico, el crimen organizado y el terrorismo internacional, se interrelacionan entre sí y en algunos casos tiene un comienzo en común.

Es por ello que estos tiempos debemos hablar de una policía judicial científica (ver título VI de mi proyecto 6.702-D-99) que entre otras, debe tener la facultad de integrar un sistema coordinado informativo investigativo con otros organismos públicos (AFIP, BCRA, Superintendencia de Seguros, entes de control de servicios públicos, oficinas de prevención, control y lucha contra el narcotráfico, registros de propiedad de cada distrito, registros de barcos y aeronaves, etcétera).

Cuando en el inciso 3 del artículo 23 del proyecto de hábeas data dice que "los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento", estamos facultando, lisa y llanamente a que las organizaciones delictivas profesionales, que atentan permanentemente contra la seguridad de la población, puedan exigir a la Policía Federal y a las policías de las provincias a que eliminen todos los datos que se colectan en la labor de inteligencia una vez finalizada la investigación instructoria. Entiéndase bien, no podemos sancionar una norma tan vaga que será rápidamente tergiversada por el crimen organizado.

En la Directiva de Protección de Datos de la Unión Europea de octubre de 1995 (95/46/EC), que constituye uno de los ordenamientos jurídicos más importantes del derecho comparado en esta materia, los europeos se esmeran principalmente en excepcionar toda la actividad de tratamiento de datos relacionada con la seguridad pública.

En el artículo 3º, apartado 2 de la directiva, se establece: "Las disposiciones de la presente Directiva no se aplicarán al tratamiento de datos personales... que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienes-

tar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del Estado en materia penal".

Esta política se aprecia en su total magnitud con la creación en 1995 de la Oficina Europea de Policía —Europol— (Diario Oficial Nº C 316 del 27-11-95, páginas 2-32). El objetivo común consiste "en lograr una mejora de la cooperación policial en el ámbito del terrorismo, del tráfico ilícito de estupefacientes y de otras formas graves de delincuencia internacional mediante un intercambio de información permanente, seguro e intensivo entre Europol y las unidades nacionales de los Estados miembros".

En el artículo 3º del Convenio Europol, se detallan las "funciones" y en especial destacamos aquellas que tienen relación con el uso de las nuevas tecnologías. "(1) facilitar el intercambio de información entre los Estados miembros; (2) recoger, compilar y analizar informaciones y datos; (3) comunicar sin demora a los servicios competentes de los Estados miembros, por medio de las unidades nacionales, los datos que les afecten y la relación entre los actos delictivos de los que hayan tenido conocimiento; (4) facilitar las investigaciones en los Estados miembros transmitiendo a las unidades nacionales toda la información pertinente al respecto; (5) gestionar sistemas informatizados de recogida de datos".

Por todo lo expuesto resulta imperioso que el inciso 3 del artículo 23 se elimine, advirtiendo, señor presidente, que en nada se mengua la tutela del ciudadano en orden a protegerlo contra abusos que pudieren cometer las mismas autoridades públicas, en este caso las fuerzas de seguridad, ya que el plexo normativo vigente en nuestro país, y el resto del articulado del proyecto de hábeas data otorgan al ciudadano una efectiva protección (artículo 4º —Calidad de datos—, 13 —Derecho de información—, 14 —Derecho de acceso—, 15 —Contenido de la información—, 16 —Derecho de rectificación, actualización o supresión—, 23 —Supuestos especiales inciso 1 y 2—, 29 —Órgano de control— y 32 —Sanciones penales—). A ello le debemos sumar el importantísimo fallo de la Corte Suprema de la Nación del 15-10-98, "Urteaga, Facundo Raúl c/Estado nacional - Estado Mayor Conjunto de las FF.AA. s/ amparo ley 16 986", que consagra vía jurisprudencial la mayoría de estos derechos.

Propuesta: se suprime el inciso 3, que dice: "3. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento".

### *Seguridad en el comercio*

La regulación de los bancos de datos de riesgo crediticio es, sin lugar a dudas, uno de los clamores públicos que aún se encuentra insatisfecho. Incurriríamos en responsabilidad grave si nuestra Honorable Cámara de Diputados deja caducar el presente proyecto de ley.

El accionar de las bases de datos comerciales ha despertado un debate inusitado desde la entrada en vigencia de la acción de hábeas data en 1994 y los tribunales han dictado una extraordinaria jurisprudencia y se ha producido una profusa doctrina que más abajo señalamos. La polémica más fuerte se ha desatado alrededor del derecho que tienen estas empresas en la conservación de información histórica en sus bases de datos con la finalidad de proteger al crédito.

Nadie duda que así debe ser, pero no menos cierto es que los deudores no deben ser medidos todos con la misma vara, máxime en un país que ha estado sujeto a sucesivas crisis económicas, en donde la buena fe de muchos consumidores que no pudieron pagar se confunde con la mala fe de otros que violentan permanentemente las buenas prácticas que deben regir en los negocios comerciales.

Es por ello que la redacción de Asuntos Constitucionales es superior a la del Senado y además recoge el derecho comparado más reciente. Me refiero a la legislación chilena que por vez primera establece una separación entre deudores morosos que refinancian y pagan de aquellos que no pagan, dentro de cuyo grupo encontramos a los individuos de mayor peligrosidad, que son aquellos que cometen fraude, quiebran dolosamente sus empresas, utilizan testaferros, fundan decenas de sociedades fantasmas para liar sus pasivos.

Y he dicho que la Honorable Cámara de Diputados supera la redacción del Senado porque automáticamente de pagada una deuda, la historia crediticia se reduce a tres años, produciendo un cambio sustancial respecto de la realidad actual que nos indica que las empresas mantienen plazos mucho más extensos de 10 años, quince otras, o bien nunca los eliminan. El plazo de tres años comulga con nuestra condición de país en vías de crecimiento, respecto de otras economías más prósperas, ya que nuestro consumidor está más expuesto a las crisis económicas que otros mercados más fuertes.

Vale citar que en los países más avanzados los plazos son mayores. En los Estados Unidos, el plazo al olvido son 7 años, excepto las quiebras, que duran 10 años por el daño social que generan. No hay derecho al olvido cuando el monto del crédito a otorgar es de u\$s 150.000 o más (artículo 605 de la Fair Credit Reporting Act de 1970). España establece 6 años para suprimir la información adversa (artículo 28 LORTAD de 1992). Brasil establece que no se pueden mantener informaciones negativas referentes a un período superior a cinco años (artículo 43, inciso 1 de la ley 8.078 de 1990). En el mismo sentido que Brasil está Dinamarca (ley 293 de 1978) Y en varios países europeos el tiempo es ilimitado, tal como en Alemania, Austria (1870), Bélgica, Finlandia, Francia, Gran Bretaña, etcétera.

El plazo de tres años permitirá una rápida inserción de la persona, que otrora fue morosa, al circuito virtuoso del crédito, con la diferencia a favor que habrá adquirido una cultura de pago más responsable

ya que cuidará su historia crediticia; porque seguramente no querrá que en su informe comercial se reflejen nuevas informaciones de morosidad que lo alejen del crédito corriente.

En este sentido, los informes crediticios son como las caras de una moneda. Mientras debemos propender a un olvido pronto luego de que se cancelen las deudas morosas, debemos proteger el derecho a la información de los ciudadanos, en especial a favor de aquellos que otorgan créditos y permitir que se recuerde a los que nunca pagan sus deudas, ya que aquí se registra un alto volumen de delincuencia de guantes blancos.

Es que en últimos años se ha revalorizado la actividad criminal vinculada a la economía. Ya en 1993, el Servicio Nacional de Inteligencia Criminal (National Criminal Intelligence Service - NCIS) del gobierno de Gran Bretaña, informó que a nivel global, las actividades desarrolladas por las organizaciones mafiosas se concentraban en la problemática de la droga sólo en un 40 %, correspondiendo el 60 % restante a actividades económicas, en un amplio rango que abarca operaciones financieras, inversiones, transacciones, fraudes y contrabando.

El peligro que implica el involucramiento de las organizaciones criminales en las actividades económicas es múltiple. Principalmente, distorsiona el normal funcionamiento de los mecanismos del mercado y la efectividad de las decisiones regulatorias emanadas de las autoridades gubernamentales. El crimen global tal como es definido por el jefe del FBI, Louis J. Freeh, es "una podrosa estructura, basada en la constante conspiración criminal y la corrupción de las instituciones estatales, financieras y económicas".

Nótese que en este contexto, el proyecto de hábeas data establece dos plazos, tres o cinco años según el deudor pague o no. Sabido es que una infinidad de deudas se pagan más allá de los cinco años, como por ejemplo las quiebras y concursos, las deudas de alto monto, la presencia de numerosos acreedores concentrados en un solo deudor con un patrimonio insuficiente, además de las deudas originadas en acciones delictuosas cuyo fin es estafar a comerciantes y consumidores de buena fe. Debemos liberar a los que pagan pero no podemos darle el mismo derecho a los cinco años a los que no pagan, sin que la deuda no esté cancelada.

Si prohibimos conocer a los que no pagan estamos dando un pésimo ejemplo a la sociedad, ya que un moroso tan sólo debe esperar dos años más respecto de otro que pagó para exigir a los bancos de datos que lo saquen de sus archivos. Y lo que es peor, estamos poniendo en serio riesgo los miles de millones de pesos que los ahorristas y las empresas confían al sistema financiero. Según la encuestas que en forma mensual aparecen en los matutinos, el nivel de depósitos alcanza aproximadamente, entre pesos y dólares, los 84.000.000 (Fundación Capital). Contrastado con la información del BCRA, que indica que el sistema presta alrededor de 72.000.000 millo-

nes, llegamos a la contundente conclusión que resulta imprescindible que el “ahorro institucional”, que las instituciones financieras presten en calidad de intermediarias, se canalice hacia tomadores que tengan suficiente capacidad de pago. Para ello la información debe ser completa, total y transparente.

Si así no fuera, estamos hipotecando uno de los pilares más sanos de la economía: el ahorro. El dinero que no retorna en forma constante y preestablecida al circuito virtuoso, produce la ruptura de la cadena de pagos y aumenta las tasas de interés, pasivas y activas, que son pagadas por los buenos pagadores.

Esta es la línea argumental que han seguido los tribunales argentinos y la doctrina mayoritaria en nuestro país. En el caso Codari s/hábeas data, se estableció que “...las dificultades financieras que podría inrogar al actor el recho de consignarse dichos datos en su legajo, no sólo resultan ajenas a la demanda, sino que se encuentran directamente vinculadas con prácticas de carácter financiero, es decir, en la medida del crédito escaso resulta lógico que los oferentes limiten sus operaciones a aquellas personas que brinden las máximas garantías de devolución del dinero prestado. De lo expuesto se condice que de hacer lugar a la pretensión de la actora implicaría por parte del suscripto una distorsión de su verdadero historial, cuyo costo, eventualmente, debería ser solventado por terceros, quienes se verían privados de tomar las decisiones referidas a sus operaciones comerciales teniendo a la vista la totalidad de los datos que puedan juzgar convenientes para aprobar o desechar una operación”.

En el caso Gorosito se agrega: “Entiendo —armonizando ambos legítimos derechos— que conocer la solvencia patrimonial del potencial cliente y su derecho a que esa información sea fidedigna se compatibiliza actualizando —sin borrar— todos los antecedentes lo que, en el subjuicio se verifica con la aclaración de que el crédito fue pagado (ver Colautti, Carlos E., “Reflexiones preliminares sobre el hábeas data”, “La Ley”, 1996-C, página 917, Mero-vich, Carina Quispe, “El hábeas data y los sistemas de información —Reflexiones acerca de la nueva garantía constitucional—”); “La Ley”, 1996-A, página 1056 (Cámara Civil Comercial de Azul, provincia de Buenos Aires, 21-5-99, “Gorosito Polonio s/hábeas data”, expediente 26.110).

En el mismo sentido, se ha resuelto que “si la información difundida por la demandada no es falsa sino que se trató de un hecho verdadero —la promoción de un juicio ejecutivo— corresponde rechazar el pedido de supresión realizado con fundamento en el artículo 43 de la Constitución Nacional, Cámara Nacional Comercial Sala C, 6-9-96, “Rodríguez, Rafael J. c/Organización Veraz S A s/sumarísimo”. “Jurisprudencia Argentina”, 1997, tomo I, página 56; Cámara Nacional Contencioso-administrativo Sala 4ª, 5-9-95, “Fairrel Desmond A., c/Banco

Central de la República Argentina y otros s/amparo ley 16.986)”, “Jurisprudencia Argentina”, 1995, tomo IV, página 350, con nota de Néstor Sagues, “Subtipos de hábeas data, a contrario sensu”: Cámara Civil y Comercial, San Isidro, Sala 1ª, 21-6-96; “De-paolini, Angela M. c/Organización Veraz S. A.”, “La Ley”, Buenos Aires, 1996, página 1082 (Cámara Civil Comercial, Azul, provincia de Buenos Aires, 21-5-99. “Gorosito Polonio s/hábeas data”, expediente 26.110)

Resulta determinante exhibir otro ejemplo proveniente de la Unión Europea. En la Directiva sobre Lucha contra la Morosidad de las Cuentas Comerciales (COM 1998-126 final 98/0099 —COD—), se establece que “La morosidad en el pago de deudas contractuales crea dificultades de tesorería y deteriora la rentabilidad y la competitividad. En los casos más graves provoca insolvencias y pérdidas de puestos de trabajo”.

“Una de cada cuatro insolvencias se debe a la morosidad. El 33 % de las empresas europeas considera la morosidad un problema grave o que amenaza la supervivencia de la empresa y dicho porcentaje alcanza el 51 % en Grecia, el 50 % en Italia y el 46 % en Francia. Con una tasa de desempleo en Europa cifrada aproximadamente en 18 millones de personas (a 1998), la morosidad constituye un problema que no puede ignorarse y que exige medidas comunitarias (Fuente: Fédération Nationale dell'Information d'Entreprises et de la Gestion de Créances —Federación Nacional de la Información a las Empresas y de la Gestión de Deudas, Lyon, septiembre de 1997— European Payment Habits Survey 1996 —Encuesta europea sobre prácticas de pago—, Intium Justitia, Amsterdam, abril de 1997—”.

“La comisión (de la Unión Europea) ha señalado reiteradamente que el riesgo de fracaso empresarial es intolerablemente alto en Europa, ya que el 50 % de las empresas no llega a superar los cinco años de vida. Puesto que la morosidad es un factor esencial en la mortalidad de las empresas, es necesario aplicar ahora todo tipo de medidas de lucha contra ella”.

“No pagar dentro de plazo constituye un incumplimiento de contrato, pese a lo cual la morosidad se ha vuelto con demasiada frecuencia la norma en vez de la excepción y los deudores se toman a la ligera el cumplimiento de sus obligaciones contractuales de pagar dentro de plazo. Los efectos perjudiciales de tales prácticas en las pequeñas y medianas empresas son especialmente graves.”

Tales normas son fundamentales a la hora de justificar la modificación que se pide, señor presidente, debemos aprovecharnos de la tradición y la experiencia comercial de vastos siglos de las naciones europeas y una de las cunas del comercio actual.

Propuesta de modificación artículo 26, inciso 4. Sólo se podrán archivar, registrar o ceder los datos personales que sean significativos para evaluar la solvencia económico-financiera de los afectados du-

rante los últimos tres años. El plazo rige desde la cancelación de la deuda (se elimina el plazo de cinco años y se deja uno solo).

Otro punto que presenta una alta confusión, es la modificación por Asuntos Constitucionales del inciso 5 del artículo 26 referido a los informes crediticios. Parece haberse confundido la fase recopilación de los datos desde las fuentes de información (A) de la fase de la venta de los mismos informes (B), regulados bajo el instituto de la cesión de datos a terceros (artículo 11 del proyecto).

Además, la actual redacción del inciso 5 no se comprende y adolece del error gramatical de *superponer dos veces el mismo condicionante "si"*, haciendo incierto el derecho de las personas a enterarse cuando son registradas en las bases de datos, al menos en este inciso.

Uno de los reclamos constantes es que las personas se ven sorprendidas de estar registradas en los informes comerciales cuando van a solicitar un crédito ya que antes desconocían que su acreedor los había denunciado como morosos. Esto tampoco está bien o está mal, es muy útil cuando se hace con responsabilidad. El proyecto prevé a través de varias normas, que los deudores, o los supuestos deudores porque a veces no lo son, tomen conocimiento en forma previa de la transmisión de sus datos y esto les permitirá realizar un control sobre la veracidad de ellos (artículo 5º —Consentimiento—, 6º —Información—, 11 —Cesión de datos— y 26 inciso 2 —Datos crediticios. Obligaciones del acreedor—).

Pero como dijimos, una cosa es la fase de recopilación (A) y otra es la fase de transmisión de esa información a los comerciantes e instituciones especializadas en el crédito —cesión de datos— (B). Las obligaciones previas de conocimiento están reguladas en el inciso 2 del citado artículo 26, y es allí donde debemos contemplar que si el acreedor no le comunicó al deudor que lo iba a denunciar a un banco de datos, sea este último el que lo haga a fin de asegurar la veracidad de los datos.

Si confundimos las fases de recopilación de datos (A) con la cesión de datos (B), corremos el peligro de sancionar una norma inconstitucional al exigir que por cada informe comercial que vendan estas empresas deba ser notificado al deudor.

Para evitar ello, se trasladan, con el mismo vocabulario, las reformas del inciso 5 al inciso 2 del artículo 26, para que con mayor claridad se enumeren las obligaciones de los acreedores que hacen uso de los bancos de datos de información crediticia.

Artículo 26, inciso 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. Los datos relacionados con el incumplimiento de obligaciones dinerarias sólo podrán tratarse si concurren los siguientes recaudos:

Apartado a): Existencia previa de una deuda cierta, vencida y exigible, que haya resultado impaga,

Apartado b): "Requerimiento previo de pago a su deudor o a quien corresponda el cumplimiento de la obligación, con la mención expresa de los servicios de información crediticia destinatarios de la información de morosidad.

Los servicios de información crediticia deberán comunicar al titular los datos de incumplimiento si se verificare que el acreedor no cumplió con el apartado anterior".

Se trasladan las modificaciones del inciso 5 de Asuntos Constitucionales al inciso 2, apartado b) y se mantiene la redacción del Senado.

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.

*Franco A Caviglia.*

#### FUNDAMENTOS DE LA DISIDENCIA DEL SEÑOR DIPUTADO FUNES

Señor presidente:

Modificaciones al despacho de Asuntos Constitucionales. (Para mayor claridad se han transcrito los textos actuales completos de los artículos o incisos en los que se propone alguna modificación. Las modificaciones o agregados mismos aparecen en letra no-grita dentro de los espacios recuadrados. Las explicaciones aparecen en letra cursiva común.)

Artículo 16, inciso 5º. Se suprime este inciso por entrar en contradicción con los anteriores, e impedir el derecho de supresión de datos, previsto por el inciso 1º de la misma norma

Artículo 26: Prestación de servicios de información crediticia Inciso 1º. 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. Inciso 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. Los datos relacionados con el incumplimiento de obligaciones dinerarias sólo podrán tratarse si concurren los siguientes recaudos:

a) Existencia previa de una deuda cierta, vencida y exigible, que haya resultado impaga;

b) Requerimiento previo y fehaciente de pago a su deudor o a quien corresponda el cumplimiento de la obligación. *En el mismo requerimiento, el acreedor deberá identificar a los servicios de información crediticia, indicando al menos domicilio y teléfono,*



c) Si el acreedor no cumple con el inciso anterior, los servicios de información crediticia deberán notificar al deudor antes de su inclusión en el banco de datos.

Inciso 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 diez años. Dicho plazo se reducirá a tres años cuando el deudor cancele o de otro modo extinga la obligación debiéndose hacer constar dicho hecho.

Inciso 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.

En este caso se vuelve a la redacción del Senado.

Artículo 27: Archivos, registros o bancos de datos con fines de publicidad.

Inciso 1: En la recopilación o cesión de datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo de bienes y servicios, no se requerirá ni el previo consentimiento ni la notificación posterior, siempre que dichos hábitos no revelen, directa o indirectamente, datos sensibles

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

Inciso 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.

Artículo 29: Órgano de control.

2. El órgano de control será el Ministerio de Economía de la Nación.

#### Disposición transitoria

Artículo 50: En el caso de la prestación de servicios de información crediticia, los acreedores que hubieren remitido información de morosidad a los bancos de datos con anterioridad a la entrada en vigencia de la presente ley, deberán controlar la información enviada con la finalidad de eliminar los errores que hubieren cometido y de actualizar las deudas que fueron canceladas. De lo contrario, quedarán expeditos a favor del titular de los datos todos los derechos que confiere esta norma, y los acreedores serán pasibles de las sanciones previstas en la presente ley.

Artículo 51: Por única vez, al promulgarse la presente ley, el plazo de diez años previsto en el inciso

4 del artículo 26 se reducirá a cinco años para las registraciones anteriores a su entrada en vigencia

Artículo 52 — De forma.

Teodoro R. Funes

#### ANTECEDENTE

Buenos Aires, 26 de noviembre de 1998

Al señor presidente de la Honorable Cámara de Diputados de la Nación.

Tengo el honor de dirigirme al señor presidente, a fin de comunicarle que el Honorable Senado, en la fecha, ha sancionado el siguiente proyecto de ley que paso en revisión a esa Honorable Cámara:

El Senado y Cámara de Diputados, ...

#### LEY DE PROTECCION DE LOS DATOS PERSONALES

##### CAPÍTULO I

##### Disposiciones generales

Artículo 1º — *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

Art. 2º — *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, orde-

nación, 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*

Art. 3º — *Archivos de datos. Licitud.* La información de archivos de datos será lícita cuando se encuentren debidamente inscritos, 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.

#### Art. 4º — *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.

#### Art. 5º — *Consentimiento.*

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

El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, juntamente con las advertencias previstas en el artículo 6º de la presente ley.

2. No será necesario el consentimiento cuando:
  - a) Los datos se obtengan de fuentes de acceso público inescrito;
  - b) Se recaben para el ejercicio de funciones propias de los poderes del Estado;
  - c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento, domicilio y número de teléfono;
  - 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.

Art. 6º — *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.

Art. 7º — *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

Art. 8º — *Datos relativos a la salud.* Los hospitales y demás instituciones sanitarias públicas o privadas y los profesionales vinculados a la ciencia médica 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.

Art. 9º — *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.

Art. 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.

Art. 11. — *Cesión.*

- 1. Los datos personales objeto de tratamiento sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés 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 5º 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.

Art 12 — *Transferencia internacional*

- 1. Es prohibida la transferencia de datos personales de cualquier tipo con países u or-

ganismos internacionales o supranacionales, que no proporcionen 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 las titulares de datos*

Art. 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.

Art. 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 estimará 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.

Art. 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 utilizan.
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, o por medios electrónicos, telefónicos, de imagen, u otro idóneo a tal fin.

Art. 16. — *Derecho de rectificación, actualización o supresión.*

1. Toda persona tiene derecho a que sean rectificadas, actualizadas 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 de 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.

Art. 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.

Art. 18. — *Comisiones legislativas.* Las comisiones de Defensa Nacional y la Comisión Bicameral de Fiscalización de los Organos y Actividad 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.

Art. 19. — *Gratuidad.* La rectificación, actualización o supresión de datos personales inexactos o incompletos se efectuará sin cargo alguno para el interesado.

Art. 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*

Art. 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.

Art. 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 establecerá el destino de los mismos o las medidas que se adopten para su destrucción.

Art. 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 aquéllos 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.

Art. 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.

Art. 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 aquél 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 cinco años.

Art. 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 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.
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.

Art. 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.

Art. 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, 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 resulta posible mantener el anonimato, se deberá utilizar una técnica de disociación, de modo que no permita identificar a persona alguna.

## CAPÍTULO V

### Control

Art. 29. — *Órgano 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 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.

Art. 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 inscritos 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

## Art. 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 (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.

## Art. 32. — Sanciones penales.

1. Incorporáse como artículo 117 bis del Código Penal, el siguiente:

- 1º 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.
- 2º 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.
- 3º La escala penal se aumentará en la mitad del mínimo y del máximo, cuando del hecho se derive perjuicio a alguna persona.
- 4º 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. Incorporáse como artículo 157 bis del Código Penal el siguiente:

Será reprimido con la pena de prisión de un mes a dos años el que:

- 1º A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales.
- 2º Revelare a otro información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley.

Quando 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

Art. 33. — *Procedencia.* 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.

Art. 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.

Quando 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.

Art. 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.

Art. 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 encuentran interconectados en redes interjurisdiccionales, nacionales o internacionales.

Art. 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 sumarisimo.

Art. 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 provisto personal 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 trata.
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.

Art. 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.

Art. 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 periódica.

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 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.

Art. 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 aquéllas 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.

Art. 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.

Art. 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.

Art. 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.

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

Art. 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.

Art. 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.

Art. 48 — Comuníquese al Poder Ejecutivo.

Saludo a usted muy atentamente.

EDUARDO MENEM.  
*Mario L. Pontaquarto.*