H. Cámara de Diputados de la Nación

Las Islas Malvinas, Georgias del Sur
y Sandwich del Sur son Argentinas

Buenos Aires, 8 de Mayo de 2002

Señor
Presidente de la H. Cámara de Diputados
Dr. Eduardo Oscar Camaño
S_____/_____**D**

De mi mayor consideración:

Me dirijo a Ud. con el objeto de solicitarle tenga a bien disponer la reproducción del proyecto, Expte Nro. 693-D-02, publicado en el Trámite Parlamentario Nro. 9 , del cual se adjuntan las copias correspondientes.
Sin otro particular, saludo a Ud. muy atte.

ELISA M. CARRIO
DIPUTADA DE LA NACION

37. **Carrió y otros**: de ley. Reproducen el proyecto de su autoría y de otros señores diputados (4.907-D.-98), de régimen de hábeas data, incorporación de los artículos 117 bis, 157 bis y 184 bis al Código Penal. Creación de la Unidad de Protección de Datos Personales (UPDP). (693-D.-2000). (Asuntos Constitucionales, Legislación Penal, Justicia y Presupuesto y Hacienda.) (Pág. 955.)

37

Buenos Aires, 4 de febrero de 2000.

Al señor presidente de la Honorable Cámara de Diputados de la Nación, don Rafael M. Pascual.

S/D.

De mi consideración:

Me dirijo a usted a los efectos de solicitarle la reproducción del expediente 4.907-D.-98. Régimen de hábeas data. Publicado en el Trámite Parlamentario Nº 109 del 10 de agosto de 1998.

Atentamente.

Elisa M. Carrió. – Mirian B. Curletti de Wajsfeld. – Angel O. Geijo.

PROYECTO DE LEY

El Senado y Cámara de Diputados,...

HABEAS DATA

CAPÍTULO I

Principios generales

Artículo 1° – *Principio general. Objetivo.* La presente ley tiene por objeto la protección integral de los datos personales de personas físicas y jurídicas tratados en registros, bancos de datos u otros medios técnicos de tratamiento de datos, automa-

tizados o no, de los sectores públicos y/o privados, con el fin de lograr que el tratamiento de los datos se realice en forma transparente y con el debido respeto dé a la reserva de la vida privada y familiar y a todos los derechos, libertades y garantías fundamentales de la persona, garantizándoles el honor y la intimidad, así como también el acceso a la información que se registre sobre ellas, de acuerdo a lo que establece el artículo 43 de la Constitución Nacional.

Art. 2° – *Definición de conceptos.* En la presente ley se entenderá por:

a) Datos personales: cualquier información concerniente a personas físicas o jurídicas determinadas o determinables. Se considerará determinable toda persona cuya identidad puede identificarse en particular, directa o indirectamente, por medio de alguno o varios de los elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social;

b) Datos sensibles: son aquellos datos personales que manifiestan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información sobre la salud o sobre la vida sexual;

c) Registro, archivo, base o banco de datos: indistintamente designan el conjunto estructurado de datos personales, que permitan el acceso de acuerdo con parámetros determinados, que sea objeto de tratamiento o procesamiento, automatizado o no, cualquiera que sea la forma o modalidad de su creación, organización, almacenamiento o acceso;

d) Tratamiento de datos: cualquier operación o conjunto de operaciones, realizadas o no mediante procedimientos automatizados que se apliquen a datos personales, que permitan o faciliten el acceso a aquéllos, el cotejo o la interconexión, el bloqueo, la eliminación o la destrucción, tales como la recogida, almacenamiento, grabación, elaboración, organización, registro, conservación, resguardo, modificación, disociación, consulta, extracción, difusión, eliminación, etcétera;

e) Responsable del registro, archivo, base o banco de datos: persona física o jurídica, de naturaleza pública o privada, que sea titular del registro, o que determine los fines y los medios del tratamiento de los datos;

f) Encargado del tratamiento: persona física o jurídica, de naturaleza pública o privada, que trate datos personales por cuenta del responsable;

g) Titular de los datos: persona física o jurídica, cuyos datos sean objeto de tratamiento de acuerdo con la definición formulada en el presente artículo;

h) Destinatario: las personas físicas o jurídicas, autoridad pública, servicio o cualquier otro organismo que reciba comunicación de datos;

i) Usuario de datos: toda persona, pública o privada, que realice tratamientos de datos, ya sea en registros, archivos, bancos o bases de datos propias o a través de conexiones;

j) Consentimiento del interesado: manifestación de voluntad, libre, específica e informada, a través de la cual, el interesado consiente el tratamiento de los datos personales que le conciernen;

k) Procedimiento de disociación de datos: tratamiento de datos personales mediante el cual se obtiene información que no puede ser asociada a una persona determinada o determinable;

l) Almacenamiento de datos: la obtención, toma o custodia de datos personales, en registros o banco de datos para su utilizació posterior;

m) Cesión de datos: la transferencia o la puesta a disposición de los datos tratados a terceros, cuando ellos son suministrados por el responsable del registro;

n) Modificación de datos: todo cambio en el contenido de datos almacenados en registros o bancos de datos;

o) Ficha personal: contenido de la información de una persona, que permite su identificación y describe sus antecedentes y actividades de cualquier tipo;

p) Interconexión de datos: forma de tratamiento de datos que consiste en la correlación de datos de un fichero con los datos de otro/s fichero/s, mantenidos por otro/s responsables o por el mismo responsable con una finalidad diferente;

q) Eliminación de datos: destrucción de datos almacenados, automatizados o no, sea cual fuere el procedimiento utilizado para ello.

Art. 3° – *Ambito de aplicación:* El régimen de protección de los datos de carácter personal que se establece en la presente ley no será de aplicación:

a) A los archivos, registros, bancos de datos de personas físicas con fines exclusivamente personales;

b) A los archivos, registros, bancos de datos de información tecnológica o comercial que reproduzcan datos ya publicados en boletines diarios o repertorios oficiales y otras publicaciones de carácter general, sin perjuicio, de la responsabilidad que podría generar la reproducción de dichos datos, conforme a lo dispuesto en la presente ley;

c) A los archivos, registros, bancos de datos de información jurídica, accesibles al público, en la medida en que se limiten a reproducir disposiciones o resoluciones judiciales publicadas en periódicos, revistas o repertorios oficiales;

d) A los archivos, registros, bancos de datos mantenidos por partidos políticos, sindicatos, de las personas físicas o jurídicas dedicadas a la actividad periodística, iglesias, confesiones o comunidades religiosas en cuanto a los datos que se refieran a sus afiliados, asociados o miembros y ex miembros, sin perjuicio de la cesión de datos que queda sometida a lo que dispone la presente ley, salvo que se trate de datos sensibles o de cualquier otro dato que posibilite procesos discriminatorios.

Se regirán por disposiciones específicas:

a) Los registros regulados por la legislación sobre régimen electoral;

b) Los derivados del Registro Nacional de Reincidencia y Estadística Criminal y el Registro Nacional de Personas;

c) Los que sirvan a fines exclusivamente estadísticos, sin perjuicio de lo dispuesto por el artículo 7°, sobre datos especialmente protegidos.

Capítulo II

Tratamiento de los datos

Art. 4° – *Calidad de los datos tratados.* Los datos de carácter personal:

a) Sólo podrán recogerse para su tratamiento cuando sean ciertos, adecuados, pertinentes y no excesivos con relación al ámbito y la finalidad legítima para las que se hubieran obtenido;

b) Deberán ser recolectados por medios leales y lícitos, por tanto, no podrán realizarse a través de medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley;

c) No podrán ser utilizados para finalidades distintas o incompatibles de aquellas para las que hubieren sido recogidos. Los fines de la recolección deben ser determinados, explícitos y legítimos;

d) Deberán ser exactos y actualizados de forma tal que respondan con veracidad a la situación real del interesado;

e) Que resulten total o parcialmente inexactos, o que sean incompletos, deberán ser eliminados y sustituidos, o en su caso completados, por el responsable del registro cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular de rectificación, actualización y eliminación. Además, se deberán tomar todas las medidas necesarias y razonables para que los datos inexactos o incompletos respecto a los fines para los que fueron recogidos o para los que fueron objeto de tratamiento, sean eliminados o rectificados;

f) Deberán ser almacenados de modo tal que permitan el ejercicio del derecho de acceso de su titular;

g) Deberán ser conservados en forma tal que permitan la identificación de los interesados durante un período no superior al estrictamente necesario para los fines que fueron recogidos;

h) Deberán ser eliminados cuando hayan dejado de ser necesarios a los fines para los cuales hubieran sido recabados.

Art. 5° – *Consentimiento/ilicitud.* El tratamiento de datos de carácter personal es ilícito cuando el titular no hubiere dado su consentimiento expreso, libre e informado. El consentimiento que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo con las circunstancias.

Cuando el titular prestare su consentimiento, juntamente con otras declaraciones se lo deberá informar de ello expresamente y por instrumento separado.

Podrá prescindirse del consentimiento cuando:

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

b) Se trate de listados cuyos datos se limiten a nombre, ocupación, fecha de nacimiento, domicilio y número de teléfono;

c) Los datos deriven de una relación contractual y resulten necesarios para su cumplimiento;

d) Los datos resulten necesarios para la protección de un interés vital del interesado y éste fuera física o legalmente incapaz de prestar su consentimiento. En dichos casos se recurrirá al consentimiento del representante legal del incapaz;

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

f) Cuando los datos fueran necesarios para la prevención de un peligro real y cierto para la defensa nacional o para la seguridad interior, mediando orden de autoridad competente.

Art. 6° – *Revocación del consentimiento.* El consentimiento podrá ser revocado en forma expresa o por otro medio que permita presumirlo fehacientemente.

Art. 7° – *Datos especialmente protegidos.*

1. Ninguna persona podrá ser obligada a proporcionar datos sensibles.
2. Queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles.
3. El tratamiento de los datos sensibles podrá permitirse cuando:

a) Sea efectuado en el curso de sus actividades legítimas y con las debidas garantías por una asociación o cualquier otro organismo sin fin de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refiera exclusivamente a sus miembros o a las personas que mantengan contactos regulares con la fundación, asociación o el organismo en razón de su finalidad y con tal de que los datos no se comuniquen a terceros sin el consentimiento expreso de los interesados;

b) El tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos, o sea necesario para el reconocimiento, ejercicio o defensa de sus derechos en un procedimiento judicial;

c) Adoptando las medidas de seguridad de la información necesaria, sea indispensable para la protección de la seguridad del Estado, la defensa, la seguridad pública y la prevención, investigación o represión de delitos penales, mediando orden de autoridad competente.

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 recabar y tratar los datos personales relativos a la salud física y mental de los pacientes que acudan a los mismos o que estén o hubieran estado bajo tratamiento de aquéllos, respetando los principios del secreto profesional.

Art. 9° – *Registro de condenas penales, medidas de seguridad e infracciones.* La creación y mantenimiento de registros relativos a condenas penales, medidas de seguridad e infracciones, sólo podrá ser realizada por autoridad pública, de forma tal que no sea violatorio de los derechos, libertades y garantías del titular de los datos.

Capítulo III

Seguridad y confidencialidad de los datos

Art. 10. – *Seguridad de los datos.* El responsable o usuario del registro o banco de datos deberá adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos de carácter personal, para evitar la adulteración, pérdida, destrucción accidental o ilícita, consulta, acceso o tratamiento no autorizado, difusión, y que a la vez permitan detectar posibles desviaciones de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

Las medidas que se adopten deberán garantizar, habida cuenta de los conocimientos técnicos existentes, del coste de su aplicación, de la naturaleza de los datos y los riesgos a los que estuvieran expuestos, un nivel de seguridad apropiado. Quedará prohibido el registro de datos de carácter personal en archivos, bases o bancos de datos que no reúnan las condiciones técnicas de integridad y seguridad mínimas e indispensables.

Art. 11. – *Medidas especiales de seguridad.* En los casos de los artículos 7°, inciso 3 *c)* y 9°, los responsables del tratamiento de los datos deberán adoptar medidas especiales de seguridad de la información.

Art. 12. – *Deber de confidencialidad.* El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales se encuentran obligados a guardar secreto profesional respecto de aquéllos. Dicha obligación subsistirá aun después de finalizada su relación con el titular del registro de datos.

Podrá ser relevado de su obligación de guardar secreto mediante resolución judicial, cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública.

Art. 13. – *Deber de confidencialidad de la autoridad de control.* La obligación enunciada en el artículo anterior también recaerá sobre los miembros de la autoridad de control, incluso después del término de su mandato, así como también sobre los funcionarios, agentes o técnicos que ejerzan funciones asesoras o de autoridad de control.

Capítulo IV

Derechos del titular de los datos

Art. 14. – *Derecho de información.* Cualquier persona podrá conocer la existencia de registros, archivos, bases o bancos de datos de carácter personal, su finalidad y la identidad del responsable. Dicha información deberá ser suministrada por el organismo de control relativo a la existencia de archivos, registros o bases o bancos de datos, que será de consulta gratuita y pública.

Art. 15. – *Derecho de información en la recolección de datos.* Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa, precisa e inequívoca:

a) La identidad y domicilio del responsable del registro;

b) Los fines del tratamiento de que van a ser objeto los datos y de la imposibilidad de modificar su finalidad;

c) Los destinatarios o las categorías de destinatarios de los datos y la imposibilidad de modificarlos;

d) El carácter obligatorio o facultativo de las respuestas al cuestionario que se les proponga y las consecuencias que podrían generarles la proporción de los mismos, la negativa a hacerlo o la inexactitud de los brindados;

e) La existencia de derechos de acceso, rectificación y eliminación de los datos que les conciernen.

Toda persona tiene derecho a ser informada antes de que los datos se comuniquen a terceros y a que se le ofrezca expresamente el derecho de oponerse a dicha comunicación o utilización.

Art. 16. – *Derecho de acceso.* El titular tiene derecho a solicitar y obtener información libremente y sin restricciones sobre los datos de carácter personal que se tengan sobre él incluidos en registros, archivos, bases o bancos de datos públicos o privados o privados destinados a proveer información. Asimismo, también tiene derecho a saber quiénes han solicitado información sobre su persona.

El requerido deberá asegurarse de la identidad del peticionante y deberá cumplir su obligación dentro de los diez días corridos de haber sido solicitada. Vencido el plazo sin que se satisfaga el pedido, o si realizado el informe se estimara que es insuficiente, quedará expedita la acción especial de amparo prevista en esta ley.

El derecho de acceso podrá ser ejercitado a intervalos no inferiores a tres meses, salvo que el peticionante acredite un interés legítimo al efecto, en cuyo caso podrá ejercerlo en cualquier momento.

Art. 17. – *Características de la información.* La información que se le facilite al peticionante, debe ser:

a) Suministrada en forma clara, inteligible, exenta de codificaciones y en caso de que las haya, deben estar acompañadas de una explicación de los términos que se utilicen; la explicación debe estar en lenguaje que sea accesible al conocimiento medio de la población;

b) Amplia y debe versar sobre la totalidad del registro perteneciente al titular incluso en los casos donde éste sólo haya requerido información sobre uno o más de los datos personales que existen sobre él, incluyendo además el origen de los datos;

c) Exclusivamente sobre los datos personales del peticionante; en el informe no podrá darse información sobre terceros, aun cuando éstos estén vinculados con el peticionante;

d) Suministrada por escrito, por medios electrónicos, telefónicamente o por cualquier otro medio idóneo a elección del titular del derecho.

Art. 18. – *Derecho de rectificación, eliminación y actualización.* Toda persona tiene derecho a que sus datos personales incluidos en registros, archivos, bases o bancos de datos sean rectificados, actualizados y en los casos en que sea necesario, eliminados o sometidos a confidencialidad.

Tanto el responsable como el usuario y el encargado del registro tendrán la obligación de hacer efectivo el derecho y proceder a la rectificación, actualización o eliminación de los datos personales del afectado. El plazo máximo para realizar dicha tarea será de cinco días hábiles de recibida la denuncia o de advertido el error o la falsedad.

El incumplimiento de dicha obligación dentro del plazo establecido en el presente artículo, habilitará al peticionante a promover directamente la acción de amparo prevista en esta ley.

Durante el plazo en el cual se desarrollará el proceso de verificación y rectificación del error o falsedad de la información, el responsable o encargado de registro deberá bloquear el archivo o aclarar, al proveer información relativa al mismo, el hecho de que se encuentra sometido a revisión.

Si los datos que fueron rectificados o eliminados hubieren sido cedidos o transferidos previamente, el responsable o el encargado del registro deberán notificar la rectificación o la eliminación efectuada al cesionario, dentro del tercer día hábil de realizado el tratamiento del dato. Si los datos hubieran sido publicados en algún medio de acceso público, deberá publicarse allí mismo la rectificación o la actualización correspondiente, dentro del tercer día hábil de realizada.

La eliminación de datos incompletos no procederá en aquellos casos en los que pudiere causarse perjuicios a derechos o intereses legítimos del afectado o de terceros, o cuando existiese una obligación legal de conservar los datos pudiéndose completar los datos faltantes.

Los datos de carácter personal deberán conservarse durante los plazos previstos en las disposiciones pertinentes aplicables o, en su caso, en las relaciones contractuales entre el responsable del registro y el interesado y mientras subsista la finalidad que lo justifica.

Art. 19. – *Excepción al derecho de acceso y/o eliminación.* Los responsables podrán excepcionalmente denegar el acceso, eliminación de datos de carácter personal cuando fuere indispensable para la protección de la seguridad pública y para la protección de los derechos de terceros. También podrá denegarse, con criterio restrictivo, cuando mediante dicha información se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a investigaciones sobre el cumplimiento de obligaciones tributarias o previsionales y el desarrollo de funciones de control de la salud y del medio ambiente. En todos estos casos, la resolución que así lo disponga deberá ser fundada y notificada al peticionante.

Sin perjuicio de lo establecido, deberá permitirse al peticionante tener acceso a los registros en todos los supuestos donde éste deba ejercer su derecho de defensa.

Al que se le negare, en forma total o parcial, el ejercicio de los derechos de acceso o eliminación, sobre la base de lo dispuesto por el presente artículo, podrá poner esta situación en conocimiento del Defensor del Pueblo o interponer acción especial del amparo.

Art. 20. – *Gratuidad.* La rectificación, actualización o eliminación de datos de carácter personal inexactos o incompletos se efectuará sin cargo alguno para el interesado.

Capítulo V

Transferencia y rotación de datos personales

Art. 21. – *Interconexión de datos personales.* La interconexión de datos personales solamente se permitirá si fuera necesaria para la consecución de finalidades legales o reglamentarias y cuando no suponga discriminación, restricción, alteración o menoscabo de derechos, libertades o garantías de los titulares de los datos.

La interconexión de datos personales deberá ser realizada de acuerdo con las medidas de seguridad previstas en la presente ley.

Art. 22. – *Cesión de datos.* Los datos de carácter personal objeto de tratamiento podrán ser cedidos exclusivamente para la satisfacción de los fines directamente relacionados con el interés legítimo del cedente y del cesionario, con el previo consentimiento expreso, libre e informado del titular de los datos. A este último se lo debe informar sobre la finalidad de la cesión y sobre la identidad de cesionario. Toda cesión donde no conste con claridad la finalidad que la ha motivado y no haya constancia del consentimiento del titular de los datos será nula. Dicho consentimiento podrá ser revocado.

El cesionario quedará sujeto a las mismas obligaciones legales y reglamentarias a las que se encuentra vinculado el cedente y éste responderá solidaria y conjuntamente por la inobservancia de aquéllas ante el organismo de control y el titular de los datos que están afectados.

Art. 23. – *Prescindencia del consentimiento.* El consentimiento no será exigido, cuando:

a) En los casos previstos en la segunda parte del artículo 5°;

b) La cesión tenga por destinarios a los magistrados del Poder Judicial, al Defensor del Pueblo o al Ministerio Público, en ejercicio de las funciones propias de su competencia;

c) La cesión se produzca entre las administraciones públicas con arreglo al artículo 26;

d) Se trate de datos personales relativos a la salud y sean necesarios para solucionar una emergencia o para la realización de estudios epidemiológicos, sin que para ello hubiera otro medio más idóneo y se requiera acceder a un registro, en tanto se preserva 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 forma tal que los titulares no sean identificables.

Art. 24. – *Cesión de datos entre administraciones públicas.* Los datos de carácter personal sometidos a tratamiento por parte de las administraciones públicas en el ejercicio de sus atribuciones, no podrán ser cedidos a otras administraciones públicas para el desempeño de competencias diferentes o que versen sobre materias distintas, excepto en aquellos casos donde la cesión haya estado prevista por las normas de creación del registro o banco de datos o por disposición posterior de igual o mayor rango.

Los datos de carácter personal que una administración pública obtenga para ser destinados a otra entidad de la administración pública podrán ser cedidos a aquélla.

Art. 25. – *Transferencia de datos. Principios.* Queda prohibida la cesión o la transmisión internacional de datos de carácter personal de cualquier tipo con países u organismos internacionales o supranacionales, que no garanticen un nivel de protección adecuado.

El carácter adecuado del nivel de protección se evaluará tomando en cuenta todas las circunstancias que concurran en una cesión o transferencia. Especialmente se tomará en consideración la naturaleza de los datos, la finalidad y la duración del/os tratamiento/s previsto/s, las normas de derecho vigentes en el país de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

Art. 26. – *Excepciones.* No obstante lo dispuesto en el artículo anterior, los Estados podrán autorizar que se realice una cesión o transferencia de datos personales a un país que no garantice un nivel de protección adecuado, cuando:

a) El interesado haya dado su consentimiento expreso, libre e informado a la transferencia prevista;

b) Sea necesaria para la colaboración judicial internacional;

c) El intercambio sea de datos de carácter médico, cuando sea necesario para el tratamiento del afectado, o para una investigación epidemiológica, en la medida que se haga de acuerdo a lo establecido en el artículo 25 inciso *e);*

d) La transferencia sea necesaria para la salvaguarda de un interés vital del interesado;

e) La transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés pú-

blico fundamental, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial;

f) La transferencia tenga carácter bancario o bursátil, en lo relativo a las transacciones respectivas y conforme a la legislación que resulte aplicable;

g) La transferencia tenga lugar desde un registro público que, en virtud de disposiciones legales o reglamentarias, esté creado para brindar información al público y esté abierto a la consulta del público en general o por cualquier persona que pueda demostrar interés legítimo, siempre que se cumplan las condiciones que establece la presente ley;

h) La transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el narcotráfico, y el lavado de dinero proveniente de ilícitos.

CAPÍTULO VI

Responsables, usuarios y tipos de registros

Art. 27. – *Principio general.* Todo archivo, registro, banco o base de datos, sea de titularidad pública o privada, destinado a proporcionar información deberá inscribirse en el Registro General de Protección de Datos.

En el registro de archivos cada uno de los responsables de los registros de datos de carácter personal completará un formulario, en el que manifestará sus datos personales, las características y finalidad del archivo, la naturaleza y el destino de los datos, medios que utilizará para garantizar la seguridad de los datos, tiempo de conservación, forma y personas que podrán acceder a ellos.

La elaboración de dicho formulario quedará en manos de la unidad de protección de datos personales (UPDP), creado por el artículo 38 de la presente ley.

En ningún registro, archivo, base o banco de datos podrán contenerse datos de carácter personal de naturaleza distinta a la declarada en el registro.

Art. 28. – *Registro de datos públicos.* La creación, modificación o eliminación de archivos, registros, banco o base de datos pertenecientes a organismos públicos sólo podrán hacerse mediante disposiciones generales –actos legislativos y administrativos correspondientes– publicados en el Boletín Oficial de la Nación, anotándose en Registro General de Protección de Datos.

Art. 29. – *Registros de titularidad privada.* Los particulares que formen archivos, registros, bancos o bases de datos que no sean exclusivamente para uso personal y contengan datos de carácter personal deberán registrarse conforme a lo previsto en el artículo 29.

Art. 30. – *Registros o banco de datos de defensa y seguridad nacional.* Los registros o bancos de datos de las fuerzas armadas y organismos de seguridad e inteligencia que contengan datos de carácter personal, que por haberse almacenado para fines administrativos deban ser objeto de registro permanente, quedarán sujetos al régimen general de la presente ley. También se aplicarán las disposiciones de la presente ley a los antecedentes personales que proporcionen dichos bancos de datos a las autoridades administrativas o judiciales que lo requieran en virtud de disposiciones legales.

El tratamiento de datos personales con fines de defensa nacional por parte de las fuerzas armadas, fuerzas y organismos de seguridad, organismos policiales o de inteligencia, sin consentimiento de los afectados, quedará exclusivamente limitado a aquellos supuestos y categorías de datos que resulten imprescindibles para la prevención de un peligro real y cierto para la defensa nacional y para la seguridad pública debiendo ser tratados en registros o banco de datos específicos y establecidos al efecto.

Los datos personales registrados con fines policiales serán eliminados cuando dejen de ser necesarios para las averiguaciones que motivaron su tratamiento.

Art. 31. – *Datos sobre los abonados al servicio de telecomunicaciones.* Los números de teléfono y demás servicios prestados por empresas de telecomunicaciones, junto con otros datos complementarios, podrán figurar en los repertorios de abonados de acceso al público, siempre que el interesado no hubiese pedido su exclusión.

Art. 32. – *Prestación de servicios de tratamiento de datos.* Cuando por cuenta de terceros se presten servicios de tratamiento de datos de carácter personal, éstos no podrán aplicarse o utilizarse con un fin distinto al que figure en el contrato de servicios, ni cederlos a terceros ni aun para su conservación.

Una vez cumplida la prestación contractual, los datos de carácter personal tratados deberán ser eliminados, salvo que existiere 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 podrán almacenar con las debidas condiciones de seguridad por un período máximo de cinco años.

Art. 33. – *Prestación de servicios sobre solvencia patrimonial y crédito.* Quienes se dediquen a la prestación de servicios de información sobre la solvencia patrimonial y el crédito sólo podrán tratar datos de carácter personal obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el afectado o con su consentimiento.

A su vez, también podrán tratarse datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones monetarias facilitadas por el acreedor o por quien actúe por su cuenta o interés. En estos casos, se notificará a los afectados respecto de los datos de carácter personal que hayan sido registrados en ficheros, en el plazo de

veinte días desde dicha registración, informándoles acerca del contenido de los datos que hubiesen sido incluidos y de su derecho a recabar información sobre la totalidad de ellos, en los términos establecidos en la presente ley.

Cuando el afectado lo solicite, el responsable o usuario del banco de datos, le comunicará las informaciones, así como las evaluaciones y apreciaciones que sobre él hayan sido comunicadas durante los últimos seis meses y el nombre y domicilio del cesionario en los supuestos en los cuales los datos hayan sido obtenidos mediante cesión.

Sólo se podrán registrar, archivar o ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económico-financiera de los afectados y que no se refieran, cuando sean adversos, a más de seis años.

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. 34. – *Prestación de servicios con fines publicitarios o análogos.* Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad o venta directa y otras actividades análogas, podrán tratar datos que sean aptos para establecer perfiles determinados con fines promo-cionales, comerciales o publicitarios; o que 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.

Los afectados podrán ejercer libremente el derecho de acceso, el que también comprenderá los datos que hubieren sido dados de baja y la fuente de donde han sido obtenidos, sin cargo alguno.

En cualquier momento, el titular podrá solicitar el retiro o eliminación de las informaciones que sobre él figuren en los registros, a su simple solicitud.

Art. 35. – *Prestación de servicios relativos a encuestas o investigaciones.* Con el fin de realizar encuestas de opinión, trabajos de prospección de mercados, investigaciones científicas o médicas y actividades análogas, siempre que los datos recogidos no pudieran atribuirse a una persona identificada o identificable, podrían no ser aplicadas las normas de la presente ley.

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 en particular. Si ello no pudiera lograrse efectivamente, se deberá requerir el consentimiento expreso, libre e informado de las afectados.

CAPITULO VII

Autoridad de control

Art. 36. – *Naturaleza.* Créase la Unidad de Protección de Datos Personales, que será un órgano independiente, con autarquía económica e independencia funcional y no estará sujeto a instrucciones y dictará su propio reglamento interno. El Registro General de Protección de Datos estará bajo la órbita de la UPDP.

Estará integrada por ocho expertos elegidos por una comisión *ad hoc* y un presidente elegido por el Congreso de la Nación mediante el voto de las dos terceras partes de sus miembros.

El organismo encargado de la selección de los miembros de la UPDP será una comisión *ad hoc* integrada de la siguiente manera:

–Dos miembros del Poder Judicial elegidos por sus pares.

–Dos funcionarios del Ministerio Público elegidos por el procurador general de la Nación.

–Cuatro representantes del Poder Legislativo respetando la representación de las minorías parlamentarias.

La selección se ajustará a las siguientes directivas:

a) Los postulantes serán seleccionados mediante concurso público de oposición y antecedentes. La comisión ad hoc convocará a concurso dando a publicidad las fechas de exámenes;

b) Previamente se determinarían los criterios y mecanismos de evaluación, y los antecedentes que serán computables;

c) La prueba de oposición procurará evaluar tanto la formación teórica como la práctica.

La comisión *ad hoc* realizará la preselección de los postulantes a integrar la UPDP a los efectos de preparar una nómina de aquellos que acrediten idoneidad suficiente para presentarse al concurso público de oposición y antecedentes.

La comisión *ad hoc* elegirá los nueve miembros titulares y los nueve miembros suplentes de la UPDP, los que durarán cuatro años en su cargo, pudiendo ser reelegidos por un período más.

Art. 37. – *Funcionamiento.* LA UPDP se reunirá en sesiones plenarias al menos cuatro veces al mes en la forma que establezca el reglamento interno. El quórum para sesionar será de cinco miembros y adoptará las decisiones por mayoría absoluta de los miembros presentes, salvo cuando esta ley prevea mayoría especial.

Art. 38. – *Remoción.* Los integrantes de la UPDP podrán ser removidos de su cargos por el voto de las dos terceras partes de los miembros totales del cuerpo, cuando incurrieren en mal desempeño de sus funciones, mediante un procedimiento que asegure el derecho de defensa del acusado.

Art. 39. – *Funciones y atribuciones.* La UPDP es la autoridad nacional cuya finalidad será controlar y fiscalizar el cumplimiento de las disposiciones legales y reglamentarias en materia de protección de datos personales, con riguroso respeto de

los derechos, libertades y garantías individuales. A tal fin, tendrá las siguientes funciones y atribuciones:.

a) Autorizar el registro de los tratamientos informatizados de datos personales;

b) Asegurar el derecho de acceso a la información, así como el ejercicio del derecho de rectificación y de actualización;

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

d) Tramitar la peticiones de cualquier persona, o que la represente, de protección de sus derechos y libertades respecto al tratamiento de datos personales e informarla del resultado de la petición;

e) Controlar la observancia de las normas sobre integridad y seguridad de datos incluido en archivos, registros, banco o bases de datos;

f) 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 de carácter personal que se les requieran;

g) Efectuar, de oficio o a petición de cualquier persona, la comprobación de la licitud de un tratamiento de datos, cuando dicho tratamiento esté sujeto a restricciones de acceso o de información; en caso de que dicha investigación se haya realizado por solicitud de tercero, deberá informarle del resultado de la misma;

h) Imponer sanciones administrativas que en su caso correspondan por violación a las disposiciones de la presente ley;

i) Realizar un censo de archivos, registros, banco o bases de datos alcanzados por la ley y mantener el registro permanente de los mismos.

Art. 40. – *Deber de colaboración.* Las entidades públicas y privadas están obligadas a prestar colaboración a la UPDP, facilitándole toda la información que les sea requerida en el ejercicio de sus competencias.

Art. 41. – *Obligación de notificación.* El responsable del tratamiento, previamente a la realización de uno o un conjunto de tratamientos total o parcialmente automatizados destinados a fines determinados, deberá notificar de ello a la UPDP.

La UPDP podrá eventualmente eximir de la obligación de notificación a determinadas categorías de tratamiento que, en función de los datos, no sean susceptibles de afectar a los derechos y libertades de los titulares de los datos. Dicha autorización deberá especificar, entre otras cosas: las finalidades del tratamiento, los datos o las categorías de datos a tratar, los destinatarios a los que podrán ser comunicados dichos datos y el período de su conservación.

Estarán exentos de la obligación de notificación, quienes realicen tratamiento de datos cuya exclusiva finalidad sea el mantenimiento de registros que se destinen a información al público o puedan ser consultadas por el público en general o por cualquier persona que demuestre un interés legítimo.

Art. 42. – *Código de conducta.* 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 de carácter personal tendientes a asegurar y mejorar las condiciones de operación de los sistemas de información, los que entre otras cosas podrán establecer las condiciones de organización, funcionamiento, normas de seguridad, programas o equipos, obligaciones de las partes intervinientes en el tratamiento de datos, garantías para el ejercicio de los derechos de los titulares de los mismos, etcétera. El contenido de ese código tipo deberá respetar cabalmente los principios establecidos en la presente ley.

Dichos códigos deberán ser inscritos en el Registro General de Datos Personales, quien podrá denegar la inscripción cuando considere que él no se adecua a las disposiciones legales y reglamentarias sobre la materia.

Capítulo VIII

Procedimiento

Art. 43. – *Principio general.* Sin perjuicio del derecho de presentación de quejas ante la UPDP, toda persona tiene derecho a acudir a los tribunales de justicia si considera que han sido violados los derechos garantizados por esta ley.

En consecuencia, la acción de *habeas data* o la acción especial de amparo de protección de datos personales procederá para tomar conocimiento de los datos personales que se encuentren almacenados en archivos, registros, banco o bases de datos, de carácter público o privado, destinados a brindar informes y su finalidad.

El titular de los datos tiene además derecho a interponer esta acción a los fines de manifestar su oposición, en los casos previstos en el artículo 7° inciso 3 *c*), en cualquier momento y por razones legítimas propias de su situación en particular, a que los datos que le conciernen sean objeto de tratamiento. En caso de oposición justificada dichos actos no podrán ser tratados.

También podrá interponerse en todos aquellos casos en donde se presuma la falsedad, inexactitud, desactualización de la información o se hayan incluido datos que tiendan a discriminar a las personas afectadas por razones de religión, raza, sexo, vida sexual, opiniones políticas, filosóficas o mora-

les, o por razones de salud para exigir su eliminación, rectificación, confidencialidad o actualización.

Art. 44. – *Procedimiento aplicable.* La acción de *habeas data* tramitará de acuerdo a las disposiciones de la presente ley y por el procedimiento que corresponda a la acción de amparo común y supletoriamente por las normas contenidas en el Código Procesal Civil y Comercial de la Nación, en lo relativo al juicio sumarísimo.

Art. 45. – *Legitimación activa.* La acción podrá ser ejercida, en caso de personas físicas, tanto por el afectado como por sus sucesores, sean éstos en línea directa o colateral hasta el segundo grado, personalmente o mediante apoderado, En los casos donde la acción sea ejercida por personas de existencia ideal, ella deberá ser interpuesta por sus representantes legales, o por sus apoderados designados a tal efecto. El Defensor del Pueblo podrá intervenir en cualquier proceso en forma coadyuvante con el consentimiento del afectado.

Art. 46. – *Competencia.* El juez del domicilio del actor, el del domicilio del demandado, o el del lugar en el que el acto se exteriorice o pudiese tener consecuencias, será el magistrado competente a elección del actor.

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

Art. 47. – *Contenido de la demanda.* La demanda será interpuesta por escrito y deberá individualizar con la mayor precisión posible el nombre y domicilio del archivo, registro, banco o base de datos, así como el nombre del responsable de él; en casos de que ellos sean públicos, se intentará establecer el organismo estatal del cual depende.

En los casos donde el peticionante además de pretender el acceso, busque la eliminación, rectificación, actualización o confidencialidad de los datos, la demanda también deberá demostrar que la información es falsa, o que es inexacta, o que es inadecuada para la finalidad alegada para justificar la creación del registro o que se trata de datos sensibles.

Art. 48. – *Trámite.* Presentada la demanda y ante el carácter manifiesto de información discriminatorio, falso o inexacto de la información, el juez podrá ordenar que se bloquee provisionalmente el registro en la parte referente a los datos personales que motivaron la acción.

Admitida la acción el juez requerirá del archivo, registro, banco o base de datos la remisión de la información concerniente al accionante. A su vez, también podrá requerir información acerca del soporte técnico de datos, documentación relativa a la recolección y sobre cualquier otro aspecto que considere procedente.

El plazo para responder el informe solicitado no podrá exceder de cinco días hábiles, el que excepcionalmente podrá ser ampliado por el juez por cinco días más.

Art. 49. – *Contestación del informe.* Al contestar el informe, el archivo, registro, banco o base de datos deberá expresar las razones por las cuales ha incluido la información cuestionada y aquéllas por las que no evacuó el pedido efectuado por el interesado, de acuerdo a los artículos 14 y 17 de la presente ley.

Art. 50. – *Confidencialidad de la información.* Los archivos, registros, banco o bases de datos privados no podrán alegar la confidencialidad de la información que se les requiere, salvo que sea un caso en el que se vean afectadas las fuentes de información periodísticas.

Los archivos, registros, banco o bases de datos públicos cuando aleguen la concurrencia de alguna de las excepciones previstas en esta ley o en una ley específica, deberán acreditar la concurrencia de los extremos que hacen aplicable la excepción legal sostenida ante el juez competente. Para ello, deberán mandarle al juez los informes requeridos, para que sea éste quien decida acerca de la correcta subsunción de la excepción legal alegada al caso particular y del carácter reservado o no del informe, decidiendo si le dará traslado o no al peticionante.

El juez deberá expedirse sobre la excepción planteada dentro del segundo día. Dicha resolución judicial podrá ser apelada dentro del segundo día de notificada. El escrito de apelación deberá ser fundado.

La apelación será denegada o concedida dentro del segundo día de planteada, con ambos efectos. En caso de ser concedida, el expediente será elevado al tribunal de alzada dentro del día de ser concedido.

Art. 51. – *Sentencia.* Una vez que el informe haya sido contesto o vencido el plazo para hacerlo y habiendo sido producida la prueba pertinente el juez dictará sentencia.

En caso de que el juez considere procedente la acción, deberá especificar si la información tendrá que ser eliminada, rectificada, actualizada o declarada confidencial, fijando un plazo dentro del cual deberá cumplirse su resolución.

En cualquier caso la sentencia se comunicará a la UPDP, el que deberá llevar un registro al efecto.

Art 52. – *Responsabilidad civil.* Toda persona que haya sufrido un perjuicio como consecuencia del tratamiento ilícito de datos o de cualquier otro acto incompatible con disposiciones legales en materia de protección de datos personales, podrá obtener del responsable del registro la reparación del perjuicio causado.

CAPÍTULO IX
Infracciones y delitos

Art. 53. – *Sanciones administrativas.* Sin perjuicio de las responsabilidades administrativas que correspondan, de la responsabilidad por daños y perjuicios derivados de la inobservancia de las normas

de la presente ley y de las sanciones penales pertinentes, la UPDP podrá aplicar la sanciones de apercibimiento, suspensión, multa de mil pesos ($ 1.000) a cuarenta mil pesos ($ 40.000), o cancelación de la autorización del registro de acuerdo con lo dispuesto por los artículos subsiguientes.

Art. 54. – *Omisión o defectuoso cumplimiento de las obligaciones.* Las entidades que, por negligencia, no cumplan con la obligación de notificar al organismo de control el tratamiento de datos personales a que hace referencia el artículo 42, presenten informaciones falsas o cumplan deficiente o parcialmente con dicha obligación, serán objeto de las siguientes multas:

a) Si se trata de personas individuales, la multa será de mil pesos ($ 1.000) a cinco mil pesos ($ 5.000);

b) Si se trata de personas colectivas o de entidades sin personalidad jurídica, será de mil quinientos pesos ($ 1.500) a siete mil quinientos pesos ($ 7.500).

Art. 55. – *Otras infracciones.* Serán objeto de sanción de multa de dos mil pesos ($ 2.000) a veinte mil pesos ($ 20.000), las entidades que no cumplan con alguna de las siguientes disposiciones:

a) Articulo 4°, calidad de los datos;

b) Articulo 10, seguridad de los datos,

c) Artículo 11, medidas especiales de seguridad;

d) Artículo 12, deber de confidencialidad,

e) Artículo 13, deber de confidencialidad de la autoridad de control;

f) Artículo 15, derecho de información en la re- colección de datos;

g) Artículo 16, derecho de acceso;

h) Artículo 18, derecho de rectificación, eliminación y conservación.

i) Artículo 22, oposición.

La multa será del doble del máximo cuando no se cumplan las obligaciones establecidas en:

a) Artículo 5°, consentimiento/ilicitud;

b) Artículo 7°, datos especialmente protegidos;

c) Artículo 8°, datos relativos a la salud,

d) Artículo 9°, registro de condenas penales, medidas de seguridad e infracciones;

e) Artículo 23, interconexión de datos personales;

f) Artículo 24, cesión de datos;

g) Artículo 26, cesión de datos entre administraciones públicas;

h) Artículo 27, cesión de datos entre registros o bancos de datos públicos;

i) Artículo 29, excepciones en la transferencia de datos.

Art. 56. – *Sanciones penales.* Incorpórese al Código Penal, como artículo 117 bis, el siguiente texto:

Será reprimido con prisión de un mes a dos años o con multa de dos mil pesos ($ 2.000) a veinte mil pesos ($ 20.000) el que insertara o hiciera insertar a sabiendas datos falsos en un archivo de datos de carácter personal;

La pena será de seis meses a tres años para el que proporcionare a un tercero a sabiendas información falsa contenida en un archivo de datos de carácter personal.

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

Cuando el autor o responsable del ilicito sea funcionario público en ejercicio de sus funciones, se le aplicará la accesoria de inhabilitación por mal desempeño de cargos públicos por el doble del tiempo de duración de la condena.

Incorpórese al Código Penal, como articulo 157 bis, el siguiente texto: Será reprimido con la pena de prisión de seis meses a tres años el que a sabiendas e ilegítimamente, violando sistemas de seguridad y confidencialidad de datos, accediere, de cualquier forma, a un banco de datos de carácter personal.

La escala penal se aumentará en la mitad del mínimo y del máximo si el acceso hubiere posibilitado al agente o a un tercero el conocimiento de datos personales.

Incorpórese al Código Penal, como articulo 184 bis, el siguiente texto: Será reprimido con la pena de prisión de tres meses a tres años el que, sin la debida autorización, destruya, cause daño o modifique datos personales, inutilizándolos o afectando su capacidad de uso.

Capítulo X

Disposiciones generales

Art. 57. – *Ambito de aplicación.* Las normas contenidas en los capítulos I, II, III, IV, V y VIII son de orden público y de aplicación en lo pertinente en todo el territorio de la Nación.

La jurisdicción federal regirá respecto de los registros, archivos, banco o bases de datos interconectados en redes de alcance interjurisdiccionales, nacionales o internacionales.

Se invita a las provincias a adherir a la normas de esta ley que fueren de aplicación exclusiva en jurisdicción nacional. Además, se las invita a crear su propios registros de bancos de datos provinciales y a establecer sus órganos de aplicación. La ausencia de reglamentación procesal no impedirá la tramitación de la acción sumarísima prevista en el artículo 43 de la Constitución Nacional.

Art. 58. – *Disposición transitoria.* Los archivos, registros, banco o bases de datos destinados a proporcionar informes existentes al momento de la sanción de esta ley, tendrán que inscribirse en el Re-

gistro General de Protección de Datos y deberán adecuarse a lo que establece el presente régimen dentro de los 180 días de creado el registro.

Art. 59. – Comuníquese al Poder Ejecutivo.

FUNDAMENTOS

Señor presidente:

El artículo 43 de la Constitución Nacional tal vez sea una de las reformas más trascendentales introducidas por la Convención Constituyente de 1994; allí no sólo se consagran expresamente las garantías individuales del hábeas corpus y el amparo, también se incorpora la figura del hábeas data.

Nuestro artículo 43 consagra una acción especial de amparo, que es conocido en el derecho comparado como hábeas data. Como vía procesal constitucional concreta ha tenido origen en la Constitución brasileña de 1988, la que siguió los lineamientos de la ley 824 de diciembre de 1984 del estado de Río de Janeiro.

En nuestro derecho público provincial no está previsto específicamente como acción judicial, pero sin embargo, muchas Constituciones se refieren al tema desde el punto de vista de fondo, enmarcándolo tanto dentro del derecho a la privacidad, como del derecho de acceso a las fuentes de información o registros de bancos de datos. Entre las primeras se encuentran la de Córdoba y Tierra del Fuego. Por otra parte, últimamente ha encontrado acogida en la Constitución de Colombia (1991), Paraguay (1992) y Perú (1993) entre otras y ha sido objeto de análisis en diversos encuentros internacionales.

Básicamente, el fundamento del hábeas data es otorgar una garantía especial al derecho a la intimidad. El derecho a la privacidad o a la intimidad, es una consecuencia o derivación del derecho a la dignidad. Por lo tanto, mediante este instrumento, se garantiza a todos los individuos el derecho a solicitar judicialmente la exhibición de los registros -públicos o privados- en los cuales están incluidos su datos personales o de los de su grupo familiar, para tomar conocimiento de su exactitud y a requerir la rectificación o supresión de datos inexactos u obsoletos o que impliquen discriminación. Esta herramienta tiende a proteger a la persona contra calificaciones sospechosas incluidas en registros, que –sin darle derecho a contradecirlas– puede llegar a perjudicarle de cualquier modo. ("Hábeas data." En La reforma constitucional, Ekmekdjian.)

El hábeas data ha nacido con el fin de intentar brindar una respuesta transaccional a los derechos constitucionales de "registrantes" y "registrados", y atiende a cuestiones de fondo (los derechos de cada uno de aquéllos) y de forma (el tipo de procedimiento para asegurar tales derechos).

Con relación a la cuestiones de fondo, el hábeas data tiene cinco fines principales: *a)* acceder a los registros de datos; *b)* actualizar los datos atrasados; *c)* corregir información inexacta; *d)* asegurar la "confidencialidad" de cierta información legalmente colectada, pero que no debería trascender a terceros; *e)* cancelar datos que hacen a la llamada "información sensible", potencialmente discriminatoria o que perfora la privacidad del registrado. C. Sagües, "Amparo, hábeas data y hábeas corpus" en La reforma constitucional.)

Es decir, el bien jurídico tutelado no sólo lo constituye sustancialmente la veracidad de la información, protegiendo a los individuos contra la información falsa o incompleta, sino concordantemente protege lo más inherente a la propia persona, que es el derecho a su perfil y el derecho a su imagen (Vanossi, "El hábeas data no puede ni debe contraponerse a los medios de prensa". "E.D").

Entonces, si se admite que la "dignidad de la persona" desde su perspectiva individual, es uno de los fundamentos últimos de todos los derechos personalísimos no cabe duda que en este caso es sustancialmente la dignidad humana como valor lo que está en la esencia de las cosas, pues la captación registral informática desnuda la personalidad psicosocial en sus aspectos más salientes, exteriores y recónditos. Son datos relacionables desde cuyo entrecruzamiento puede accederse a la personalidad completa virtual, abarcando todos los bienes de la persona de una vez: intimidad, imagen, honor, cuerpo, salud y libertad, patrimonio. (Cifuentes, "Derecho personalísimo a los datos personales".)

De antaño los datos más entrañables de las personas se registran, se archivan y se comunican dándolos a conocer. Sin embargo, es la base de datos informática la que ha traído una reacción proteccional de la persona relacionada con esos almacenamientos testimoniales. La informática, en realidad, no ha agregado nada a la operación de acumular la historia personal y patrimonial de cada uno, ni al contenido o sustancia de registros tan complejos, variados y numerosos. Es sólo un instrumento nuevo para acopiarlos, pasando del soporte de cartón o papel de fichas, libros, cuadernos y hojas, películas, fotocopiado y cintas, a la memoria de los ordenadores computarizados en donde se incorporan, se relacionan y duermen ahora los datos, o reviven a voluntad del que opera con ellos. (Cifuentes, "Protección inmediata de los datos privados de la persona. Hábeas data operativo", "La Ley", 1995-E.)

Sin embargo, la irrupción de la informática ha replanteado la cuestión del derecho a la intimidad, el derecho a la dignidad, en atención al riesgo que para la persona, implica la estructuración de grandes bancos de datos de carácter personal, y particularmente la potencialidad del entrecruzamiento de la información contenida en los mismos.

Mediante la informática se han podido crear grandes bancos de datos que permite una gran concentración de enormes volúmenes de información de carácter personal, permitiendo que sean rápida y fá-