



CM/ 331

Presidencia de la República Oriental del Uruguay

MINISTERIO DEL INTERIOR

MINISTERIO DE RELACIONES EXTERIORES

MINISTERIO DE ECONOMIA Y FINANZAS

MINISTERIO DE DEFENSA NACIONAL

MINISTERIO DE EDUCACION Y CULTURA

MINISTERIO DE TRANSPORTE Y OBRAS PUBLICAS

MINISTERIO DE INDUSTRIA, ENERGIA Y MINERIA

MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL

MINISTERIO DE SALUD PUBLICA

MINISTERIO DE GANADERIA, AGRICULTURA Y PESCA

MINISTERIO DE TURISMO Y DEPORTE

**MINISTERIO DE VIVIENDA, ORDENAMIENTO TERRITORIAL Y MEDIO
AMBIENTE**

MINISTERIO DE DESARROLLO SOCIAL

Montevideo, 16 SET. 2007

Señor Presidente de la

Asamblea General

El Poder Ejecutivo tiene el honor de dirigirse a ese Cuerpo a los efectos de someter a su consideración el Proyecto de Ley que se acompaña.

Con la amplia difusión de las tecnologías de la información y las comunicaciones, el tratamiento de los datos personales se encuentra en una situación de tensión. Ésta deriva del valor asociado a las bases de datos personales -en virtud de los potenciales beneficios, producto de su uso en actividades económicas, políticas o sociales-, al tiempo que las personas titulares de los datos tienen derecho a conocer el tratamiento al que están siendo sometidos sus datos personales y preservar su privacidad.

El presente proyecto de ley de protección de datos personales tiene como objeto establecer un marco jurídico claro y necesario para garantizar y hacer efectivo uno de los derechos fundamentales del ser humano, como es el del derecho a la protección de los datos de carácter personal y por tanto de la intimidad de las personas.

El artículo 72 de la Constitución establece: "La enumeración de derechos, deberes y garantías hecha por la Constitución, no excluye los otros que son inherentes a la personalidad humana o se derivan de la forma republicana de gobierno".



Se desprende de este artículo 72 que el Derecho a la Protección de Datos Personales es un derecho inherente a la persona humana, siendo por tanto un derecho fundamental con rango constitucional, que debe ser tutelado y garantizado especialmente por el Estado.

Tengamos en cuenta que la libertad de expresión se compone de dos derechos fundamentales: la libertad de opinión y la libertad de información. La libertad de opinión y de conciencia implica el derecho a no ser molestado ni discriminado por las ideas o creencias personales.

La libertad de información o informática aparece como un nuevo derecho de autotutela de la propia identidad, o sea el derecho de controlar (conocer, corregir, quitar o agregar) los datos personales inscriptos en un fichero.

El proyecto tiene la característica de incluir a todos los datos personales, a diferencia de la ley 17.838 que regula en exclusividad los datos destinados a brindar informes de carácter comercial, manteniéndose el marco regulatorio de los mismos.

Referente al proceso de Habeas Data podemos cotejarlo con el Habeas Corpus y vemos que existe una coincidencia en cuanto a la naturaleza jurídica, ya que no se trata de derechos fundamentales, sino de instrumentos o garantías procesales de defensa de los derechos a la libertad personal (habeas corpus) y de la libertad informática (habeas data). El procedimiento propuesto incorpora algunas modificaciones al vigente, que entendemos mejora y esclarece algunos aspectos del mismo, y lo convierte en una herramienta útil, ya se trate de habeas data propio o impropio.

Nuestro país necesita contar con una normativa como la prevista, no solo en cuanto a la regulación específica de los derechos que constitucionalmente poseen los ciudadanos, sino también en el relacionamiento con terceros países.

El presente marco normativo, permitiría a Uruguay encuadrar dentro de los requerimientos de la Unión Europea como país seguro en cuanto al envío de datos, ya que los elementos considerados a tales efectos son: en primer lugar, asegurar un nivel satisfactorio de cumplimiento de las normas, lo que presupone la existencia de una ley de protección de datos, que se posea un órgano de control y un régimen sancionatorio. En segundo lugar la posibilidad de ofrecer apoyo y asistencia a los interesados en el ejercicio de sus derechos. Esto presupone la existencia de un organismo que entre sus tareas incluya: asesoramiento a los ciudadanos sobre sus derechos, campañas de difusión sobre los derechos sobre los datos personales y cursos formativos para profesionales y/o titulares de bases de datos. En tercer lugar ofrecer vías adecuadas de recurso a quienes resulten perjudicados en el caso de que no se observen las normas, tanto en vía administrativa (ante el organismo de control) como en vía jurisdiccional (acción de habeas data).

Sin entrar a valorar los aspectos relativos a la defensa de los derechos humanos, desde el punto de vista estrictamente económico, ser un país con nivel de protección de datos personales no adecuado, constituye una potencial barrera no arancelaria para el acceso a mercados y para la captación de inversiones, particularmente aquellos pertenecientes a la Unión Europea.

La adecuación permitiría la captación de inversiones en el sector tecnológico y de servicios provenientes de países que exigen el nivel de protección de datos personales explicitado.



Presidencia de la República Oriental del Uruguay

Por otra parte en el marco de la Reforma del Estado es necesario garantizar el uso adecuado de datos personales en un contexto donde se incrementará en forma significativa el intercambio electrónico de datos entre los diferentes organismos del Estado.

Resumen del proyecto

El proyecto de ley de Protección de Datos Personales está estructurado en los siguientes capítulos:

- I. Disposiciones generales
- II. Principios Generales
- III. Derechos de los titulares de los datos
- IV. Datos especialmente protegidos
- V. Ficheros de titularidad pública
- VI. Ficheros de titularidad privada
- VII. Órgano de Control
- VIII. Acción de Protección de Datos Personales
- IX. Disposiciones transitorias

En el capítulo primero se establece el objetivo del presente proyecto de ley, que consiste en reconocer legislativamente el derecho fundamental a la protección de datos personales reconocido en el artículo 72 de nuestra Constitución.

Tiene además, como objeto proteger los datos personales, garantizando el derecho al honor y a la libertad de las personas y el acceso a la información que sobre las mismas se registre.

El capítulo segundo consagra los principios generales en materia de protección de datos, que son: juridicidad, veracidad, finalidad, previo consentimiento informado, seguridad de los datos, reserva y responsabilidad.

Los derechos de los titulares de los datos se encuentran regulados en el capítulo III, reconociendo los siguientes derechos: a la información, a la información durante la recolección de los datos, de acceso, a la rectificación, actualización y la eliminación o supresión de los datos, a la impugnación de valoraciones personales y referentes a la comunicación de los datos.

Se dedica el capítulo IV a la protección de los datos sensibles, realizando un marco para los datos relativos a la salud, a las telecomunicaciones, a ficheros con fines de publicidad, a la actividad comercial o crediticia y a la transferencia internacional de datos.

Los capítulos V y VI refieren a la regulación de los ficheros de titularidad pública y privada respectivamente.



En el capítulo VII se establece que el Órgano de Control en esta materia será una Unidad Reguladora y de Control de Datos Personales, la cual funcionará en forma desconcentrada de la AGESIC, definiendo los cometidos y estableciendo las potestades sancionatorias de la misma.

El capítulo VIII establece las acciones procesales para efectivizar la protección de los datos regulada en la ley.

Finalmente, el capítulo IX establece el régimen transitorio y el traslado del régimen actual y órgano de control de los datos comerciales, incluyéndolos dentro del régimen general.

El Poder Ejecutivo saluda a ese Cuerpo con la mayor consideración,

Dr. Tabaré Vázquez
Presidente de la República



Presidencia de la República Oriental del Uruguay

PROYECTO DE LEY

CAPITULO I – DISPOSICIONES GENERALES

Artículo 1º. Derecho Humano Fundamental.

El derecho a la protección de datos personales es inherente a la persona humana, según lo reconoce el artículo 72 de la Constitución de la República.

Artículo 2º Objeto.

La presente ley tiene por objeto garantizar y proteger los datos personales de personas físicas y jurídicas asentados en bases de datos, sean estos públicos o privados.

Artículo 3º. Ámbito de aplicación.

El régimen de la presente ley:

3.1 Será de aplicación a los datos personales registrados en cualquier soporte, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los ámbitos público o privado.

3.2 No será de aplicación a las siguientes bases de datos:

- a) A los mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
- b) Los que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado y sus actividades en materia penal, investigación y represión del delito.
- c) A las bases de datos creadas y reguladas por leyes especiales.

Artículo 4º. Definiciones.

A los efectos de la presente ley se entiende por:

- a) Consentimiento del titular: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual el titular consienta el tratamiento de datos personales que le concierne.
- b) Comunicación de datos: toda revelación de datos realizada a una persona distinta del titular de los datos.
- c) Dato personal: información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables.
- d) Dato sensible: datos personales que revelan origen racial y étnico, preferencias políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud, a la vida sexual y a toda otra zona reservada a la libertad individual.



- e) Destinatario: persona física o jurídica, pública o privada, que recibiere comunicación de datos, se trate o no de un tercero.
- f) Disociación de datos: todo tratamiento de datos personales de manera que la información obtenida no pueda vincularse a persona determinada o determinable.
- g) Encargado del tratamiento: persona física o jurídica, pública o privada que sola o en conjunto con otros trate datos personales por cuenta del responsable de la base de datos o tratamiento.
- h) Base 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.
- i) Fuentes accesibles al público: aquellas bases de datos cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación.
- j) Tercero: la persona física o jurídica, pública o privada, distinta del titular del dato, del responsable de la base de datos o tratamiento, del encargado y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable o del encargado del tratamiento.
- k) Responsable de la base de datos o tratamiento: persona física o jurídica, pública o privada, propietaria de la base de datos o que decida sobre la finalidad, contenido y uso del tratamiento.
- l) Titular de los datos: Persona cuyos datos sean objeto de un tratamiento incluido dentro del ámbito de acción de la presente Ley.
- m) Tratamiento de datos: operaciones y procedimientos sistemáticos de carácter automatizado o no, que permitan el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.
- n) Usuario de datos: toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en una base de datos propia o a través de conexión con los mismos.

CAPITULO II – PRINCIPIOS GENERALES

Artículo 5º. Valor y fuerza.

La actuación de los responsables de las bases de datos, tanto públicos como privados, y, en general, de todos quienes actúen en relación a datos personales de terceros, deberá ajustarse a los siguientes principios generales:

- a) legalidad;
- b) veracidad;
- c) finalidad;
- d) previo consentimiento informado;
- e) seguridad de los datos;
- f) reserva; y
- g) responsabilidad.



Presidencia de la República Oriental del Uruguay

Dichos principios generales servirán también de criterio interpretativo para resolver las cuestiones que puedan suscitarse en la aplicación de las disposiciones pertinentes.

Artículo 6º. Principio de legalidad.

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

Las bases de datos no pueden tener finalidades contrarias a las leyes o a la moral pública.

Artículo 7º. Principio de veracidad

7.1 Los datos personales que se recogieren a los efectos de su tratamiento deberán ser veraces, adecuados, ecuánimes y no excesivos en relación con la finalidad para la cual se hubieren obtenido. La recolección de datos no podrá hacerse por medios desleales, fraudulentos, abusivos, extorsivos o en forma contraria a las disposiciones de la presente ley.

7.2 Los datos deberán ser exactos y actualizarse en el caso de que ello fuere necesario. Los datos total o parcialmente inexactos o incompletos, deben ser en su caso suprimidos, sustituidos o completados, por datos veraces y actualizados por el responsable de su tratamiento en cuanto tenga conocimiento de dichas circunstancias. Asimismo, deberán ser eliminados aquellos datos que hayan caducado de acuerdo a lo previsto en la presente ley.

Artículo 8º. Principio de finalidad

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

8.2 Los datos deberán ser eliminados cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubieren sido recolectados.

8.3 Tampoco podrán comunicarse datos entre bases de datos, sin que medie ley o previo consentimiento informado del titular.

Artículo 9º. Principio del previo consentimiento informado

9.1. El tratamiento de datos personales de personas físicas es ilícito cuando el titular no hubiere prestado su consentimiento libre, previo, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias. Para el caso de las personas jurídicas, deberá requerirse autorización de los representantes con facultades suficientes, o de sus titulares.

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 12º de la presente ley.

9.2. No será necesario el previo consentimiento cuando:

a) Los datos provengan de fuentes públicas de información, tales como registros p, o publicaciones en medios masivos de comunicación;



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 en el caso de personas físicas a nombres y apellidos, documento de identidad, nacionalidad y fecha de nacimiento; y en el caso de personas jurídicas, razón social, nombre de fantasía, registro único de contribuyentes, domicilio, teléfono e identidad de las personas a cargo de la misma.

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

e) Se realice por personas físicas o jurídicas, privadas o públicas para su uso exclusivo personal o doméstico.

Artículo 10°. Principio de seguridad de los datos

10.1 El responsable o usuario de la base de datos debe adoptar las medidas técnicas y organizativas que resultaren 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 permitieren detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

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

10.3 Queda prohibido registrar datos personales en bases de datos que no reúnan condiciones técnicas de integridad y seguridad.

Artículo 11°. Principio de reserva

11.1 Aquellas personas físicas o jurídicas que obtuvieren legítimamente información proveniente de una base de datos que les brinde tratamiento, están obligadas a utilizarla en forma reservada y exclusivamente para las operaciones habituales de su giro o actividad, estando prohibida toda difusión de la misma a terceros.

11.2 Las personas que por su situación laboral u otra forma de relación con el responsable de una base de datos tuvieren acceso o intervengan en cualquier fase del tratamiento de datos personales, están obligadas a guardar estricto secreto profesional sobre los mismos (artículo 302 del Código Penal), cuando hayan sido recogidos de fuentes no accesibles al público. Lo previsto no será de aplicación en los casos de orden de la Justicia competente, de acuerdo con las normas vigentes en esta materia o si mediare consentimiento del titular.

Esta obligación subsistirá aun después de finalizada la relación con el responsable de la base de datos.

Artículo 12°. Principio de responsabilidad.

El responsable de la base de datos es responsable de la violación de las disposiciones de la presente ley.



Presidencia de la República Oriental del Uruguay

CAPITULO III – DERECHOS DE LOS TITULARES DE LOS DATOS

Artículo 13º. Derecho de información frente a la recolección de datos.

Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa, precisa e inequívoca:

- a) La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios;
- b) La existencia de la base 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 sensibles;
- d) Las consecuencias de proporcionar los datos, de la negativa a hacerlo o su inexactitud;
- e) La posibilidad del titular de ejercer los derechos de acceso, rectificación y supresión de los datos.

Artículo 14º. Derecho de acceso.

Todo titular de datos personales que previamente acredite su identificación con el documento de identidad o poder respectivo, tendrá derecho a obtener toda la información que sobre sí mismo se halle en bases de datos públicas o privadas. Este derecho de acceso sólo podrá ser ejercido en forma gratuita a intervalos de seis meses, salvo que se hubiere suscitado nuevamente un interés legítimo de acuerdo con el ordenamiento jurídico.

Cuando se trate de datos de personas fallecidas, el ejercicio del derecho al cual refiere este artículo, corresponderá a cualesquiera de sus sucesores universales, cuyo carácter se acreditará por la sentencia de declaratoria de herederos.

La información debe ser proporcionada dentro de los cinco días hábiles de haber sido solicitada. Vencido el plazo sin que el pedido sea satisfecho o si fuera denegado por razones no justificadas de acuerdo con esta ley, quedará habilitada la acción de habeas data.

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.

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.

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

Artículo 15º. Derecho de rectificación, actualización o supresión.



Toda persona física o jurídica tendrá derecho a solicitar la rectificación, actualización o supresión de los datos personales que le corresponda incluidos en un base de datos, al constatar error o falsedad en la información de la que es titular..

El responsable de la base de datos o tratamiento deberá proceder a realizar la rectificación, actualización, o supresión, mediante las operaciones necesarias a tal fin en un plazo máximo de cinco días hábiles de recibida la solicitud por el titular del dato o, en su caso, informar de las razones por las que estime no corresponde.

El incumplimiento de esta obligación por parte del responsable de la base de datos o tratamiento o el vencimiento del plazo, habilitará al titular del dato a promover la acción de habeas data prevista en esta ley.

No procede la eliminación o supresión de datos personales salvo en aquellos casos de notorio error o falsedad, se pueda causar perjuicio a los derechos o intereses legítimos de terceros o cuando contravenga lo establecido por una obligación legal.

Durante el proceso de verificación o rectificación de datos personales, el responsable de la base de datos o tratamiento ante el requerimiento de terceros para acceder a informes sobre los mismos, deberá dejar constancia que dicha información se encuentra sometida a revisión.

En el supuesto de comunicación, o transferencia de datos, el responsable de la base de datos o tratamiento debe notificar la rectificación o supresión al destinatario dentro del quinto día hábil de efectuado el tratamiento del dato.

La rectificación, actualización, eliminación o supresión de datos personales cuando corresponda, se efectuará sin cargo alguno para el titular.

Artículo 16º. Derecho a la impugnación de valoraciones personales

16.1 Las personas tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinado a evaluar determinados aspectos de su personalidad.

16.2 El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos personales que ofrezca una definición de sus características o personalidad.

16.3 En este caso, el afectado tendrá derecho a obtener información del responsable de la base de datos sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión manifestada en el acto.

16.4 La valoración sobre el comportamiento de las personas, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado.

Artículo 17º. Derechos referentes a la comunicación de datos

17.1 Los datos personales objeto de tratamiento sólo podrán ser comunicados para el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y del destinatario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la comunicación e identificar al destinatario o los elementos que permitan hacerlo.



Presidencia de la República Oriental del Uruguay

17.2 El previo consentimiento para la comunicación es revocable.

17.3 El previo consentimiento no será necesario cuando:

a) Así lo disponga una ley de interés general;

b) En los supuestos del artículo 9 de la presente ley;

c) Se trate de datos personales relativos a la salud y sea necesario por razones de salud e higiene públicas, 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;

d) Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos no sean identificables.

17.4 El destinatario quedará sujeto a las mismas obligaciones legales y reglamentarias del emisor 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.

CAPITULO IV – DATOS ESPECIALMENTE PROTEGIDOS

Artículo 18º. Datos sensibles

18.1 Ninguna persona puede ser obligada a proporcionar datos sensibles. Estos solo podrán ser objeto de tratamiento con el consentimiento expreso y escrito del titular.

18.2 Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley, o cuando el organismo solicitante tenga mandato legal para hacerlo. También podrán ser tratados con finalidades estadísticas o científicas cuando se disocien de sus titulares.

18.3 Queda prohibida la formación de bases de datos que almacenen información que directa o indirectamente revele datos sensibles. Se exceptúan aquellos que posean los partidos políticos, sindicatos, iglesias, confesiones religiosas, asociaciones, fundaciones y otras entidades sin fines de lucro, cuya finalidad sea política, religiosa, filosófica, sindical, que hagan referencia al origen racial, a la salud y a la vida sexual, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio que la comunicación de dichos datos precisará siempre el previo consentimiento del titular del dato.

18.4 Los datos personales relativos a la comisión de infracciones penales, civiles o administrativas sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas, sin perjuicio de las autorizaciones que la ley otorga u otorgare. Nada de lo establecido en esta ley impedirá a las autoridades públicas comunicar o hacer pública la identidad de las personas físicas o jurídicas que estén siendo investigadas por, o hayan cometido, infracciones a la normativa vigente, en los casos en que otras normas lo impongan o en los que lo consideren conveniente.

Artículo 19º. Datos relativos a la salud.



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

Artículo 20º. Datos relativos a las telecomunicaciones.

Los operadores que exploten redes públicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar, en el ejercicio de su actividad, la protección de los datos personales conforme a la presente ley.

Asimismo, deberán adoptar las medidas técnicas y de gestiones adecuadas para preservar la seguridad en la explotación de su red o en la prestación de sus servicios, con el fin de garantizar sus niveles de protección de los datos personales que sean exigidos por la normativa de desarrollo de esta ley en esta materia. En caso de que exista un riesgo particular de violación de la seguridad de la red pública de comunicaciones electrónicas, el operador que explote dicha red o preste el servicio de comunicaciones electrónicas informará a los abonados sobre dicho riesgo y sobre las medidas a adoptar.

La regulación contenida en esta ley se entiende sin perjuicio de lo previsto en la normativa específica sobre telecomunicaciones relacionadas con la seguridad pública y la defensa nacional.

Artículo 21º. Datos relativos a bases de datos con fines de publicidad

21.1 En la recopilación de domicilios, reparto de documentos, publicidad, venta u 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.

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

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

Artículo 22º. Datos relativos a la actividad comercial o crediticia

22.1 Queda expresamente autorizado el tratamiento de datos personales destinados a brindar informes objetivos de carácter comercial, incluyendo aquellos relativos al cumplimiento o incumplimiento de obligaciones de carácter comercial o crediticia que permitan evaluar la concertación de negocios en general, la conducta comercial o la capacidad de pago del titular de los datos, en aquellos casos en que los mismos sean obtenidos de fuentes de acceso público o procedentes de informaciones facilitadas por el acreedor o en las circunstancias previstas en la presente ley. Para el caso de las personas jurídicas, además de las circunstancias previstas en la presente ley, se permite el tratamiento de toda información autorizada por la normativa vigente.

22.2 Los datos personales relativos a obligaciones de carácter comercial de personas físicas sólo podrán estar registrados por un plazo de cinco años contados desde su incorporación. En



Presidencia de la República Oriental del Uruguay

caso que al vencimiento de dicho plazo la obligación permanezca incumplida, el acreedor podrá solicitar al responsable de la base de datos, por única vez, su nuevo registro por otros cinco años. Este nuevo registro deberá ser solicitado en el plazo de treinta días anteriores al vencimiento original. Las obligaciones canceladas o extinguidas por cualquier medio, permanecerán registradas, con expresa mención de este hecho, por un plazo máximo de cinco años, no renovable, a contar de la fecha de la cancelación o extinción.

22.3 Los responsables de las bases de datos se limitarán a realizar el tratamiento objetivo de la información registrada tal cual ésta le fuera suministrada, debiendo abstenerse de efectuar valoraciones subjetivas sobre la misma.

22.4 Cuando se haga efectiva la cancelación de cualquier obligación incumplida registrada en una base de datos, el acreedor deberá en un plazo máximo de cinco días hábiles de acontecido el hecho, comunicarlo al responsable de la base de datos o tratamiento correspondiente. Una vez recibida la comunicación por el responsable de la base de datos o tratamiento, éste dispondrá de un plazo máximo de tres días hábiles para proceder a la actualización del dato, asentando su nueva situación.

Artículo 23º. Datos transferidos internacionalmente

23.1 Se prohíbe la transferencia de datos personales de cualquier tipo con países u organismos internacionales, que no proporcionen niveles de protección adecuados, de acuerdo a los estándares del Derecho Internacional o Regional en la materia.

23.2 La prohibición no regirá en los siguientes supuestos:

- a) Cooperación judicial internacional;
- b) Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado por razones de salud o higiene públicas;
- 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 Oriental del Uruguay 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.

CAPITULO V – BASES DE DATOS DE TITULARIDAD PÚBLICA

Artículo 24º. Creación, modificación o supresión.

La creación, modificación o supresión de base de datos pertenecientes a organismos públicos deberán registrarse conforme lo previsto en el capítulo siguiente.

Artículo 25º. Base de datos correspondientes a las Fuerzas Armadas, Organismos Policiales o de Inteligencia



25.1 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, 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.

25.2 El tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, organismos policiales o inteligencia, sin previo consentimiento de los titulares, 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. Las bases de datos, en tales casos, deberán ser específicas y establecidas al efecto, debiendo clasificarse por categorías, en función de su grado de fiabilidad.

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

Artículo 26°. Excepciones a los derechos de acceso, rectificación y cancelación

26.1 Los responsables de las bases de datos que contengan los datos a que se refieren los apartados 25.2 y 25.3 del artículo anterior podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.

26.2 Los responsables de las bases de datos de la Hacienda Pública podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el apartado anterior cuando el mismo obstaculice las actuaciones administrativas tendientes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el titular del dato esté siendo objeto de actuaciones inspectivas.

26.3 El titular del dato al que se deniegue total o parcialmente, el ejercicio de los derechos mencionados en los apartados anteriores podrá ponerlo en conocimiento del Órgano de Control, quien deberá asegurarse de la procedencia o improcedencia de la denegación.

Artículo 27°. Excepciones al derecho a la información.

Lo dispuesto en la presente ley no será aplicable a la recolección de datos, cuando la información del titular, afecte a la defensa nacional, a la seguridad pública o a la persecución de infracciones penales.

CAPITULO VI – BASES DE DATOS DE TITULARIDAD PRIVADA

Artículo 28°. Creación, modificación o supresión.

Las personas físicas o jurídicas privadas que creen, modifiquen o supriman bases de datos de carácter personal, que no sean para un uso exclusivamente individual o doméstico, deberán registrarse conforme lo previsto en el artículo siguiente.

Artículo 29°. Inscripción registral



Presidencia de la República Oriental del Uruguay

29.1 Toda base de datos pública o privada debe inscribirse en el Registro que al efecto habilite el Órgano de Control.

29.2 Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que deberá contener la inscripción, entre los cuales figurarán necesariamente los siguientes:

- a) Identificación de la base de datos y el responsable de la misma;
- b) Naturaleza de los datos personales que contiene;
- c) Procedimientos de obtención y tratamiento de los datos;
- d) Medidas de seguridad y descripción técnica de la base de datos;
- e) Protección de datos personales y ejercicio de derechos;
- f) Destino de los datos y personas físicas o jurídicas a las que pueden ser transmitidos;
- g) Tiempo de conservación de los datos;
- h) 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.
- i) Cantidad de acreedores personas físicas que hayan cumplido los 5 años previstos en el art. 22 de la presente ley.
- j) Cantidad de cancelaciones por incumplimiento de la obligación de pago si correspondiera, de acuerdo a lo previsto en el artículo 22 de la presente ley.

29.3 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 la presente ley.

29.4 Respecto a las bases de datos de carácter comercial ya inscriptos en el Órgano Regulador, se estará a lo previsto en la presente ley respecto del plazo de adecuación.

Artículo 30°. Prestación de servicios informatizados de datos personales

30.1 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.

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



CAPITULO VII – ORGANO DE CONTROL

Artículo 31º. Órgano de Control.

31.1 Créase como órgano desconcentrado de la Agencia para el Desarrollo del Gobierno Electrónico y Sociedad de la Información (AGESIC), dotado de la más amplia autonomía técnica, la Unidad Reguladora y de Control de Datos Personales.

31.2 La Unidad Reguladora y de Control de Datos Personales estará dirigida por un Consejo integrado por tres miembros: el Director Ejecutivo de la AGESIC y dos miembros designados por el Poder Ejecutivo entre personas que, por sus antecedentes personales, profesionales y conocimiento en la materia, aseguren independencia de criterio, eficiencia, objetividad e imparcialidad en su desempeño.

Durarán tres años en el ejercicio de sus cargos, pudiendo ser designados nuevamente, y permaneciendo en ellos hasta que sean nombrados quienes hayan de sustituirlos.

31.3 La presidencia del Consejo será rotativa anualmente entre los dos miembros designados por el Poder Ejecutivo para dicho órgano y tendrá a su cargo la representación del mismo y la ejecución de las actividades necesarias para el cumplimiento de sus resoluciones.

Artículo 32º. Cometidos.

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 las bases de datos alcanzados por la ley y mantener el registro permanente de los mismos;
- d) Controlar la observancia de las normas sobre integridad, veracidad y seguridad de datos por parte de los responsables de las bases de datos, pudiendo a tales efectos realizar las actuaciones de inspección pertinentes.
- 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) Emitir opinión toda vez que le sea requerida por las autoridades competentes, incluyendo solicitudes relacionadas con el dictado de sanciones administrativas que correspondan por la violación a las disposiciones de esta ley, de los reglamentos o de las resoluciones que regulan el tratamiento de datos personales comprendidos en ésta;
- g) Asesorar en forma necesaria al Poder Ejecutivo en la consideración de los proyectos de ley que refieran total o parcialmente a protección de datos personales.



Presidencia de la República Oriental del Uruguay

h) Informar a cualquier persona sobre la existencia de bases de datos personales, sus finalidades y la identidad de sus responsables, en forma gratuita

Artículo 33°. Potestades sancionatorias

El órgano de control podrá aplicar las siguientes medidas sancionatorias a los responsables de las bases de datos o encargados del tratamiento de datos personales en caso que se violen las normas de la presente ley:

1. Apercibimiento;
2. Multa de hasta quinientas mil unidades indexadas;
3. Clausura de la base de datos respectiva. A tal efecto se faculta a la AGESIC a promover ante los órganos jurisdiccionales competentes, la clausura, hasta por un lapso de seis días hábiles, de las personas físicas o jurídicas que dispongan de bases de datos respecto de los cuales se comprobare que infringieren o transgredieren la presente ley.

Los hechos constitutivos de la infracción serán documentados de acuerdo a las formalidades legales y la clausura deberá decretarse dentro de los tres días siguientes a aquél en que la hubiere solicitado la AGESIC, la cual quedará habilitada a disponer por sí la clausura si el Juez no se pronunciare dentro de dicho término.

En este último caso, si el Juez denegare posteriormente la clausura, ésta deberá levantarse de inmediato por la AGESIC.

Los recursos que se interpongan contra la resolución judicial que hiciere lugar a la clausura, no tendrán efecto suspensivo.

Para hacer cumplir dicha resolución, la AGESIC podrá requerir el auxilio de la fuerza pública.

La competencia de los Tribunales actuantes se determinará por las normas de la Ley Orgánica de la Judicatura, N° 15.750, de 24 de junio de 1985, sus modificativas y concordantes.

Artículo 34°. Códigos de conducta

34.1 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.

34.2 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.

CAPITULO VIII – ACCION DE PROTECCION DE DATOS PERSONALES

Artículo 35°. Habeas Data.



Toda persona tendrá derecho a entablar una acción judicial efectiva para tomar conocimiento de los datos referidos a su persona y de su finalidad y uso, que consten en bases de datos públicos o privados; y -en caso de error, falsedad, prohibición de tratamiento, discriminación o desactualización- a exigir su rectificación, supresión o lo que entienda corresponder. Cuando se trate de datos personales cuyo registro esté amparado por una norma legal que consagre el secreto a su respecto, el Juez apreciará el levantamiento del mismo en atención a las circunstancias del caso.

Artículo 36º. Procedencia.

El titular de datos personales podrá entablar la acción de protección de datos personales o habeas data, contra todo responsable de una base de datos pública o privada, en los siguientes supuestos:

36.1 Cuando quiera conocer sus datos personales que se encuentran registrados en una base de datos o similar y dicha información le haya sido denegada, o no le hubiese sido proporcionada por el responsable de la base de datos, en las oportunidades y plazos previstos por la ley; o

36.2 Cuando haya solicitado al responsable de la base de datos o tratamiento su rectificación, actualización, eliminación o supresión y éste no hubiese procedido a ello o dado razones suficientes por las que no corresponde lo solicitado, en el plazo previsto al efecto en la ley.

Artículo 37º. Legitimación.

La acción de habeas data podrá ser ejercida por el propio afectado titular de los datos o sus representantes, ya sean tutores o curadores y, en caso de personas fallecidas, por sus sucesores universales, en línea directa o colateral hasta el segundo grado, por sí o por medio de apoderado.

En el caso de personas jurídicas, la acción deberá ser interpuesta por sus representantes legales o los apoderados designados a tales efectos.

Artículo 38º. Procedimiento.

Las acciones que se promuevan por violación a los derechos contemplados en la presente ley se registrarán en lo general por las normas del Código General del Proceso y en particular por las previstas en los artículos que siguen al presente, teniendo las normas procesales vigentes el carácter de supletorias en los casos de oscuridad o insuficiencias de éstas.

Artículo 39º. Trámite de primera instancia

39.1 Salvo que la acción fuera manifiestamente improcedente, en cuyo caso el Tribunal la rechazará sin sustanciarla y dispondrá el archivo de las actuaciones, se convocará a las partes a una audiencia pública dentro del plazo de tres días de la fecha de la presentación de la demanda.

39.2 En dicha audiencia se oirán las explicaciones del demandado, se recibirán las pruebas y se producirán los alegatos. El Tribunal, que podrá rechazar las pruebas manifiestamente impertinentes o innecesarias, presidirá la audiencia so pena de nulidad, e interrogará a los



Presidencia de la República Oriental del Uruguay

testigos y a las partes, sin perjuicio de que aquéllos sean, a su vez, repreguntados por los abogados. Gozará de los más amplios poderes de policía y de dirección de la audiencia.

39.3 En cualquier momento podrá ordenar diligencias para mejor proveer.

39.4 La sentencia se dictará en la audiencia o a más tardar, dentro de las veinticuatro horas de su celebración. Sólo en casos excepcionales podrá prorrogarse la audiencia por hasta tres días.

39.5 Las notificaciones podrán realizarse por intermedio de la autoridad policial. A los efectos del cómputo de los plazos de cumplimiento de lo ordenado por la sentencia, se dejará constancia de la hora en que se efectuó la notificación.

Artículo 40. Medidas provisionales.

Si de la demanda o en cualquier otro momento del proceso resultare, a juicio del Tribunal, la necesidad de su inmediata actuación, éste dispondrá, con carácter provisional, las medidas que correspondieren en amparo del derecho o libertad presuntamente violados.

Artículo 41. Contenido de la sentencia.

La sentencia que haga lugar al habeas data deberá contener:

- a) La identificación concreta de la autoridad o el particular a quien se dirija y contra cuya acción, hecho u omisión se conceda el habeas data.
- b) La determinación precisa de lo que deba o no deba hacerse y el plazo por el cual dicha resolución regirá, si es que corresponde fijarlo.
- c) El plazo para el cumplimiento de lo dispuesto, que será fijado por el Tribunal conforme las circunstancias de cada caso, y no será mayor de 15 días corridos e ininterrumpidos, computados a partir de la notificación.

Artículo 42. Recurso de apelación y segunda instancia

42.1 En el proceso de habeas data sólo serán apelables la sentencia definitiva y la que rechaza la acción por ser manifiestamente improcedente.

42.2 El recurso de apelación deberá interponerse en escrito fundado, dentro del plazo perentorio de tres días. El Tribunal elevará sin más trámite los autos al superior cuando hubiere desestimado la acción por improcedencia manifiesta, y lo sustanciará con un traslado a la contraparte, por tres días perentorios, cuando la sentencia apelada fuese la definitiva.

42.3 El Tribunal de Alzada resolverá en acuerdo, dentro de los cuatro días siguientes a la recepción de los autos. La interposición del recurso no suspenderá las medidas de amparo decretadas, las cuales serán cumplidas inmediatamente después de notificada la sentencia, sin necesidad de tener que esperar el transcurso del plazo para su impugnación.

Artículo 43. Sumariedad. Otros aspectos

43.1 En los procesos de habeas data no podrán deducirse cuestiones previas, reconveniones ni incidentes. El Tribunal, a petición de parte o de oficio, subsanará los vicios de procedimiento,



asegurando, dentro de la naturaleza sumaria del proceso, la vigencia del principio de contradictorio.

43.2 Cuando se plantee la inconstitucionalidad por vía de excepción o de oficio (arts. 509 num. 2º y 510 num. 2º del Código General del Proceso) se procederá a la suspensión del procedimiento sólo después que el Magistrado actuante haya dispuesto la adopción de las medidas provisorias referidas en la presente ley o, en su caso, dejando constancia circunstanciada de las razones de considerarlas innecesarias.

CAPITULO IX - DISPOSICIONES TRANSITORIAS

Artículo 44º. Adecuación de las bases de datos. Las bases de datos, deberán adecuarse a la presente ley dentro del plazo de un año de su entrada en vigor.

Artículo 45º. Traslado del órgano de control referente a datos comerciales.

Se establece el plazo de treinta días corridos para que el actual órgano de control en materia de protección de datos comerciales, a cargo del Ministerio de Economía y Finanzas realice el traslado de la información y documentación a la AGESIC.

Artículo 46º. Derogación.

Se deroga la Ley 17.838 de 24 de setiembre de 2004.

Artículo 47º. Reglamentación.

El Poder Ejecutivo deberá reglamentar la presente ley dentro de los ciento ochenta días de su promulgación.