MENSAJE DE S.E. LA PRESIDENTA DE LA REPUBLICA CON EL QUE INICIA UN PROYECTO DE LEY INTRODUCE MODIFICACIONES A LA LEY N° 19.628 Y A LA LEY N° 20.285.

SANTIAGO, agosto 26 de 2008.-

M E N S A J E Nº 687-356/

Honorable Cámara de Diputados:

A S.E. EL

PRESIDENTE

DE LA H.

CÁMARA DE

DIPUTADOS.

Tengo el honor de someter a vuestra consideración, un proyecto de ley que ley introduce modificaciones a la ley N° 19.628 y a la ley N° 20.285.

I. DERECHO A LA VIDA PRIVADA Y DEBER DE REGULACIÓN.

1. Derecho a la vida privada.

La Constitución, garantiza el derecho a la vida privada. En su artículo 19 N° 4, garantiza “el respeto y protección a la vida privada y pública y a la honra de la persona y de su familia.”.

Tradicionalmente se ha entendido que la vida privada se contrapone a la vida pública.

Sin embargo, qué debe atenderse por vida privada y vida pública constituye un campo difuso; además, su concepción se enlaza con el continuo y rápido avance de las tecnologías y los consiguientes cambios sociales que inciden en la configuración de la garantía.

Con todo, en relación al respeto y protección de la vida privada se pueden diferenciar dos aspectos de protección. Un aspecto negativo y uno positivo.

En su aspecto negativo, el clásico, la protección de la vida privada se caracteriza como un derecho destinado a proteger a las personas de intromisiones ilegítimas en su esfera íntima. Por ello, el derecho a la vida privada, en su dimensión de privacidad, comprende la intimidad. En este sentido, vida privada equivale a una inmunidad.

En su aspecto positivo, en cambio, la protección de la vida privada va mucho más allá, y consiste en la posibilidad de conocer, acceder y controlar las informaciones concernientes al propio individuo.

En efecto, el aspecto positivo del derecho a la vida privada se articula sobre la idea de control, mientras el aspecto negativo lo hace sobre la idea de exclusión. Por eso algunos autores distinguen entre derecho a la vida privada física y derecho a la vida privada informativa. Mediante el primero, se protege la libertad frente a toda intromisión sobre uno mismo, su casa, su familia o relaciones. Mediante el derecho a la vida privada informativa, se determina por cada sujeto cómo y en qué medida se puede comunicar a otros, información sobre uno mismo. En este último sentido, implica la facultad del individuo, derivada de la idea de autodeterminación, de decidir básicamente por sí mismo cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida (Murillo Lucas, Pablo, La protección de los datos personales ante el uso de la informática, en Estudios en homenaje al profesor don Luis Sánchez Agesta, Revista Facultad de Derecho, Universidad Complutense (RFDUC), Madrid, 1989. p. 605-606).

2. El derecho a la vida privada como garantía de autodeterminación.

La faz activa de protección de la vida privada, concebida como una facultad de control sobre la propia información, constituye hoy un elemento esencial y de gran interés en relación al ejercicio de dicho derecho, pues en este ámbito se construye la dimensión social de la personalidad.

En este contexto, el tratamiento de la información personal, datos personales, reviste gran importancia. Al respecto, existen dos modelos de derecho comparado que recogen este tema, ambos con énfasis en la protección. Por una parte, el modelo norteamericano, bajo la idea de *privacy of autonomy,* como un derecho contenido en la noción de vida privada. Por otra parte, encontramos el modelo alemán, que regula los derechos envueltos en este tratamiento, como derecho a la autodeterminación informativa, derivado del derecho a la libre autodeterminación.

En nuestro país, este derecho también ha sido analizado. Se ha señalado que “este derecho constituye la facultad de la persona de disponer de la información personal privada, íntima o sensible, que debe ser protegida por el orden social y regulada por el ordenamiento jurídico. (…) La autodeterminación informativa es la facultad de la persona concernida por los datos, almacenados en un archivo o base de datos público o privado, para autorizar su recolección, conservación, uso y circulación, como asimismo, para conocerla, actualizarla, rectificarla o cancelarla.” (Nogueira Alcalá, Humberto, “Reflexiones sobre la constitucionalización del habeas data y el proyecto de ley en tramitación parlamentaria sobre esta materia”, en Revista Ius et Praxis, año 3, N° 1, U de Talca, 1997).

3. Autodeterminación informativa como derecho de tercera generación.

Como señalara Pérez Luño (Pérez Luño, Antonio, Los derechos humanos en la sociedad tecnológica, en Libertad infromática, Leyes de Protección d Datos Personales, Cuadernos y Debates, Centro de Estudios Constitutionales, Ma-

drid, 1989, p. 143 y ss.), el derecho a la autodeterminación informativa es un derecho de tercera generación. Los derechos de primera generación fueron los derechos de defensa; los derechos de segunda generación, fueron los económicos, sociales y culturales; y los de tercera generación corresponden a los derechos que responden al fenómeno conocido como “contaminación de libertades”, atendiendo a la erosión y degradación que aqueja a los derechos fundamentales ante determinados usos de las nuevas tecnologías.

En efecto, las nuevas facetas de la vida privada propia de las sociedades avanzadas, requieren nuevos instrumentos de tutela jurídica, en especial respecto del tratamiento de los datos de carácter personal.

Se ha discutido si se trata de un derecho autónomo o de la especificación de un derecho existente (el derecho a la vida privada). Con todo, cabe señalar que la protección de la persona en materia de bases de datos y tratamientos automatizados, no puede polarizarse exclusivamente en una amenaza para la intimidad o la vida privada, pues ella constituye también un peligro para otras libertades (Pérez Luño, Antonio, Los derechos humanos en la sociedad tecnológica, en Libertad informática, Leyes de Protección d Datos Personales, Cuadernos y Debates, Centro de Estudios Constitucionales, Madrid, 1989, p. 143 y ss).

En definitiva, entonces, la pluralidad de manifestaciones de la vida privada no implica una disolución del concepto unitario de vida privada, sino más bien, su ampliación y adaptación a las exigencias de un mundo en constante cambio. Las sociedades actuales precisan de un equilibrio entre el creciente flujo de información y la garantía de vida privada de los ciudadanos.

4. La autodeterminación informativa como garantía institucional.

Este derecho comprende una serie de deberes positivo de los poderes públicos e instituciones privadas que procedan al tratamientos de datos personales. Este derecho tiene por objeto

garantizar la facultad de las personas para conocer y acceder a las informaciones que les conciernen, lo que implica la posibilidad de corregir o cancelar los datos inexactos o indebidamente procesados, y disponer su transmisión.

La protección de los datos carecería de sentido si no se tradujera en una conjunto de garantías para las personas; pero el derecho a la autodeterminación informativa sería inconcebible de no contar como presupuesto con un marco organizativo de la información (Pérez Luño, Antonio, Op. Cit., p. 141).

En otras palabras, la autodeterminación informativa no es sólo un derecho para los ciudadanos, sino también un deber para los poderes públicos e instituciones privadas. En esta parte, el legislador cumple un rol fundamental, pues tiene el deber de adoptar las medidas necesarias para proteger este derecho frente a los ataques de terceros, sin contar para ello con la voluntad de sus titulares.

II. LOS PRINCIPIOS DE LA ACTUAL REGULACIÓN.

En la actualidad, el tratamiento de datos personales y la consiguiente protección al derecho a la autodeterminación informativa se encuentra regulada en la ley N° 19.628. Dicha ley, se originó por moción parlamentaria en 1993 y vino a salvar el vacío normativo sobre la materia.

En efecto, dicha ley, consagró un conjunto de principios a los cuales debe ajustarse la recolección y tratamiento de datos personales.

1. El principio del consentimiento del afectado.

En primer lugar, la ley señala que el titular de los datos es la persona natural a la que se refieren los datos de carácter personal (art. 2 letra ñ)). En segundo lugar, la ley establece un principio general: el tratamiento de los datos personales sólo puede efectuarse cuando disposiciones legales lo autoricen o el titular consienta expresamente en ello. La ley,

a su vez, precisa que la autorización puede ser revocada por escrito y sin efecto retroactivo.

2. El principio de los datos especialmente protegidos.

La ley trata de un modo especial a los datos sensibles. Estos son una especie de dato personal.

En efecto, la ley define los datos de carácter personal o datos personales, como los relativos a cualquier información concerniente a personas naturales, identificadas o identificables. Datos sensibles, por su parte, los define como aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual (art. 2 letra f) y g)).

Ahora bien, la ley establece como principio general que este tipo de datos que no pueden ser objeto de tratamiento. Sin embargo, da tres excepciones: cuando la ley lo autorice; cuando exista consentimiento del titular; y se trate de datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares (art. 10).

3. El principio de la calidad de los datos.

El tercer principio que regula las bases de datos es su calidad. La ley parte de la base que la información que obra en las bases de datos debe ser exacta, actualizada y responder con veracidad a la situación real del titular de los datos (art. 9).

Para ello, por una parte, define el dato caduco, y por otra, diseña varios instrumentos para resguardar este principio.

En primer lugar, los datos personales deben ser eliminados o cancelados cuando su almacenamiento carezca de fundamento legal o cuando hayan caducado. Cabe señalar que la eliminación o cancelación de datos, es la destrucción de

datos almacenados en registros o bancos de datos, cualquiera fuere el procedimiento empleado para ello (art. 2 letras d) y h)). En segundo lugar, los datos han de ser modificados cuando sean erróneos, inexactos, equívocos o incompletos. En tercer lugar, deben bloquearse los datos personales cuya exactitud no pueda ser establecida o cuya vigencia sea dudosa y respecto de los cuales no corresponda la cancelación (art. 6).

Para reafirmar la calidad de los datos, la ley señala que los datos personales deben utilizarse sólo para los fines para los cuales hubieren sido recolectados, salvo que provengan o se hayan recolectado de fuentes accesibles al público.

4. El principio de seguridad.

La ley expresa este principio, por ejemplo, a través del procedimiento de disociación de datos. Este es todo tratamiento de datos personales que garantice que la información que se obtenga no pueda asociarse a persona determinada o determinable (art. 2 letra l)).

También la ley busca este objetivo estableciendo que el responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección, debe cuidar de ellos con la debida diligencia, haciéndose responsable de los daños (art. 11).

5. El principio de secreto.

Este principio lo recoge la ley al disponer que las personas que trabajan en el tratamiento de datos personales, tanto en organismos públicos como privados, están obligadas a guardar secreto sobre los mismos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público, como asimismo sobre los demás datos y antecedentes relacionados con el banco de datos. Dicha obligación no cesa por haber terminado sus actividades en ese campo (art. 7).

6. El principio de cesión.

De acuerdo a este principio, los datos que existan en una base, pueden darse a conocer. La ley define la comunicación o transmisión de datos como dar a conocer de cualquier forma los datos de carácter personal a personas distintas del titular, sean determinadas o indeterminadas (art. 2 letra c)). La comunicación puede surgir a consecuencia de una iniciativa del responsable de la base o a requerimiento.

En tal sentido, por una parte, el responsable del registro o banco de datos personales puede establecer un procedimiento automatizado de transmisión, siempre que se cautelen los derechos de los titulares y la transmisión guarde relación con las tareas y finalidades de los organismos participantes.

El receptor sólo puede utilizar los datos personales para los fines que motivaron la transmisión. Con todo, la ley se encarga de establecer dos excepciones en que no se aplican las reglas anteriores. Por una parte, cuando se trate de datos personales accesibles al público en general. Por la otra, cuando se transmiten datos personales a organizaciones internacionales en cumplimiento de lo dispuesto en los tratados y convenios vigentes (art. 5).

III. LOS DERECHOS QUE ESTABLECE LA ACTUAL REGULACIÓN.

Los titulares de los datos personales registrados en bancos de datos tienen, de acuerdo a la actual regulación, derechos para asegurar los principios recién señalados.

Estos derechos son:

1. Derecho de información y acceso.

En primer lugar, toda persona tiene derecho a exigir a quien sea responsable de un banco que se dedique en forma pública o privada al tratamiento de datos personales, información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las perso-

nas u organismos a los cuales sus datos son transmitidos regularmente.

Si los datos personales están en un banco de datos al cual tienen acceso diversos organismos, el titular puede requerir información a cualquiera de ellos (art. 14).

Cabe señalar que fuentes accesibles al público, son los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes (art. 2 letra i)).

2. Derecho de rectificación.

En segundo lugar, está el derecho a la rectificación.

La modificación de datos la define la ley como todo cambio en el contenido de los datos almacenados en registros o bancos de datos (art. 2 letra j)).

Este derecho surge respecto de los datos personales erróneos, inexactos, equívocos o incompletos, y así se acredite (art. 12 inc. 2).

3. Derecho de cancelación.

El tercer derecho del titular de los datos, es el derecho de cancelación.

Las causales que hace procedente este derecho es, por una parte, en caso que el almacenamiento de datos carezca de fundamento legal o cuando estuvieren caducos.

Por la otra, igual exigencia de eliminación, o de bloqueo de los datos, surge cuando se hubieren proporcionado voluntariamente los datos personales o ellos se usen para comunicaciones comerciales y no se desee continuar figurando en el registro respectivo, sea de modo definitivo o temporal.

Con el propósito de asegurar la efectividad de este derecho, la ley estableció tres garantías.

En primer lugar, la información, modificación o eliminación de los datos, es absolutamente gratuita, debiendo proporcionarse, además, a solicitud del titular, copia del registro alterado en la parte pertinente.

Si se efectúan nuevas modificaciones o eliminaciones de datos, el titular puede obtener, sin costo, copia del registro actualizado, siempre que haya transcurrido a lo menos seis meses desde la precedente oportunidad en que hizo uso de este derecho.

El derecho a obtener copia gratuita sólo puede ejercerse personalmente.

La segunda garantía consiste en que si los datos personales cancelados o modificados hubieren sido comunicados previamente a personas determinadas o determinables, el responsable del banco de datos debe avisarles a la brevedad posible la operación efectuada. Si no es posible determinar las personas a quienes se les comunicó, debe poner un aviso que pueda ser de general conocimiento para quienes usen la información del banco de datos (art. 12).

La tercera garantía consiste en que el derecho de las personas a la información, modificación, cancelación o bloqueo de sus datos personales, no puede ser limitado por medio de ningún acto o convención (art. 13).

Sin embargo, la ley se preocupa de establecer datos al margen de este derecho. En efecto, no puede solicitarse información, modificación, cancelación o bloqueo de datos personales, cuando ello impida o entorpezca el debido cumplimiento de las funciones fiscalizadoras del organismo público requerido, o afecte la reserva o secreto establecidos en disposiciones legales o reglamentarias, la seguridad de la Nación o el interés nacional (art. 15).

4. Derecho de indemnización.

Un cuarto derecho es a obtener una indemnización. En efecto, la persona natural o jurídica privada o el organismo público responsable del banco de datos personales, debe indemnizar el daño patrimonial y moral que cause por el tratamiento indebido de los datos, sin perjuicio de proceder a eliminar, modificar o bloquear los datos de acuerdo a lo requerido por el titular o, en su caso, lo ordenado por el tribunal.

La acción consiguiente puede interponerse conjuntamente con la reclamación destinada a establecer la infracción. Se sujeta al procedimiento sumario.

En el juicio, el juez debe tomar todas las providencias que estime convenientes para hacer efectiva la protección de los derechos que la ley establece. La prueba se aprecia en conciencia.

El monto de la indemnización debe ser establecido prudencialmente por el juez, considerando las circunstancias del caso y la gravedad de los hechos (art. 23).

IV. RAZONES DEL CAMBIO.

Pese a que la ley constituyó un gran aporte sobre la materia, su normativa ha demostrado ser insuficiente.

Paradojalmente, la ley N° 19.628, puso énfasis en el derecho a tratar datos de carácter personal y no reconoció como primer derecho, el derecho de los titulares de datos personales a controlar los mismos.

1. Regulación insuficiente.

La regulación de la actual ley ha sido criticada. Entre las principales críticas, se han señalado: la inexistencia de un registro de responsables privados de bases de datos y de un órgano fiscalizador autónomo; haber establecido que la regla general fuera que la información fuese pública y que no requiriese de la autori-

zación de sus titulares para procesarse; el no haber prohibido la transferencia internacional de datos personales a terceros países que no posean un adecuado sistema de protección; no haber otorgado protección a personas jurídicas; y de no haber exigido autorización para un cúmulo de actividades relacionadas con el tratamiento de datos personales, entre otras.

2. Necesidad de una autoridad de control.

Para velar por el adecuado cumplimiento de las disposiciones de relativas al tratamiento de datos, se requiere de una autoridad dotada de competencias y herramientas eficaces, tanto para dictar normativa sobre la materia, fiscalizar, adoptar medidas de resguardo y, en última instancia, sancionar los incumplimientos.

Sin embargo, la ley N° 19.628 no contempló un organismo administrativo, agencia o superintendencia estatal que se encargara de velar por el cumplimiento de sus normas, limitándose a entregar al Registro Civil e Identificación, el deber de llevar un registro de las bases de datos a cargo de organismos públicos. Ello ha hecho que en la práctica sea imposible fiscalizar el cumplimiento de las normas de la ley, y muchas de sus disposiciones se han tornado fútiles.

3. Necesidad de adecuarse a estándares internacionales.

Por otra parte, es necesario adecuar nuestro ordenamiento jurídico a las recomendaciones de la OCDE (Organización para la Cooperación y el Desarrollo Económico), en materia de protección de datos personales, con el fin de adecuar los estándares de nuestro país. Asimismo, es necesario cumplir con el estándar de protección de datos personales de la Unión Europea.

4. Cumplimiento de un acuerdo.

Considerando la necesidad de dar respuesta a las exigencias de protección del derecho a la autodeterminación informativa, sumado a la conciencia de que el establecimiento de una autoridad de control es fundamental para el real

cumplimiento de la ley, se planteó la necesidad de incorporar facultades en esta dirección dentro de las competencias del Consejo para la Transparencia, durante la discusión parlamentaria de la ley N° 20.285.

Sin embargo, sólo se incorporó la facultad de “Velar por el adecuado cumplimiento de la ley Nº 19.628, de protección de datos de carácter personal, por parte de los órganos de la Administración del Estado”. Se tuvo conciencia de que ello sería insuficiente para el resguardo del tratamiento de los datos personales y los derechos de los titulares. Pero se concordó en avanzar y profundizar la actual regulación.

V. DESCRIPCIÓN DE LA PROPUESTA.

Teniendo en cuenta todo lo señalado anteriormente, el presente proyecto tiene por objeto modificar dos cuerpos normativos. Por una parte, la ley N° 19.628 sobre protección de la vida privada y, por otra, la ley N° 20.285, de transparencia de la función pública y de acceso a la información de la Administración del Estado.

Con ello, se pretende dar una eficaz respuesta a las exigencias de protección, ya que, por una parte, se mejoran los estándares de protección y resguardo de los derechos de los titulares de datos personales y, por otra, se confieren las competencias y herramientas necesarias a una autoridad autónoma para velar por el adecuado cumplimiento de las normas sobre protección de datos.

1. Reconocimiento explícito de derechos.

En primer lugar, se propone consagrar explícitamente el derecho de las personas a controlar sus datos, en el art. 1° de la ley. En la actualidad únicamente se hace referencia al derecho a efectuar tratamiento de datos personales, con referencia a que tal tratamiento debe respetar los derechos de los titulares.

2. Se amplía el margen de sujetos protegidos.

En segundo lugar, el proyecto parte de la base que la información sobre las personas jurídicas es tan relevante como la de las personas naturales y también merece ser resguardada.

De ahí que el proyecto considere como legitimados activos del derecho de acceso y titulares del habeas data tanto a las personas naturales como a las jurídicas. Ambas pueden verse afectadas por un tratamiento errado o doloso de sus antecedentes personales. Y no existe razón de peso alguna para privarlos del mecanismo jurídico y procesal mediante el cual puedan obtener la corrección, actualización, modificación o eliminación de sus datos en los supuestos previstos en esta ley.

3. Establecimiento de una autoridad de control.

En tercer lugar, el proyecto establece que la autoridad encargada de velar por el cumplimiento de la normativa, tanto la contenida en esta ley, como en otros cuerpos normativos, será el Consejo para la transparencia, creado por la ley N° 20.285. Por ello, dicho Consejo pasa ahora a denominarse “Consejo para la transparencia y protección de datos personales”.

Este órgano autónomo tendrá entre sus funciones, por de pronto, mantener un Registro Único Nacional de las Bases de Datos. Enseguida, le corresponderá fiscalizar el cumplimiento de las disposiciones sobre tratamiento de datos personales, pudiendo recabar, en cualquier momento, del responsable del respectivo registro o banco de datos, la información que estime pertinente. También tiene la facultad de inspeccionar los registros o bancos de datos personales a efectos de verificar el cumplimiento de las obligaciones que establece la ley; requerir la inscripción de los bancos de datos, que no estén registrados, en el Registro Único Nacional. Un tercer tipo de potestad es la normativa. De ahí que se le faculte para dictar instrucciones de carácter general o particular, respecto de las condiciones de legitimi-

dad de un tratamiento de datos. En cuarto lugar, se le faculta para conocer de las reclamaciones de particulares relacionadas con el ejercicio de sus derechos, señalados en la ley N° 19.628 y en otras normas sobre protección de datos personales, sin perjuicio de las facultades de otras autoridades públicas. En quinto lugar, se le entregan potestades sancionadoras. Así, podrá sancionar a los responsables de los bancos de datos que infrinjan la normativa sobre protección de datos. En sexto lugar, se le faculta para requerir a los responsables y encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de esta ley y, en su caso, ordenar la cesación de los tratamientos y cancelación del registro, cuando no se ajuste a sus disposiciones. En séptimo lugar, podrá ejercer facultades en beneficio directo de las personas. En este sentido, podrá proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal y promover el respeto de los mismos; ejercer el control y adoptar las autorizaciones que procedan para las transferencias internacionales de datos, conforme lo establecido en la ley N° 19628; así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales. Finalmente, se le obliga a entregar una cuenta anual sobre la actividad desarrollada en torno a la protección de datos personales.

4. Se distingue entre encargado y responsable de la base de datos.

En cuarto lugar, el proyecto distingue entre encargado y responsable de tratamiento de datos personales, entendiendo por el primero la persona física o jurídica, autoridad pública, servicio o cualquier tercero que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento. Esta distinción permite evitar que los responsables del tratamiento de datos puedan eludir el cumplimiento de sus obligaciones.

5. Fortalecimiento de derechos de información.

En quinto lugar, se amplía el contenido de la obligación de informar al titular en la recolección de datos (artículo 3° y 3° bis).

Respecto de recolecciones de datos que se realice a través de encuestas, estudios de mercado o sondeos de opinión pública u otros instrumentos semejantes, además del carácter obligatorio o facultativo de las respuestas, se deberá informar de las consecuencias jurídicas de su negativa, la finalidad para la cual se está solicitando la información, los destinatarios de los datos y la posibilidad de que éstos sean comunicados a terceros.

Además, respecto de toda solicitud de datos personales ahora deberá informarse de forma expresa, precisa, clara e inequívoca, las siguientes circunstancias al titular de los datos:

a. Existencia del banco de datos en que se consignará su información, finalidad de la recogida de información y destinatarios.

b. Carácter obligatorio o facultativo de la entrega de sus datos y las consecuencias de su entrega o de la negativa a suministrarlos.

c. Los derechos que le asisten en virtud de la ley, especialmente el derecho de acceso, rectificación, cancelación y bloqueo.

d. El derecho a revocar su autorización para el tratamiento de los datos que le conciernen y las consecuencias de ello.

e. Una dirección física o electrónica válida en la cual pueda ejercer los derechos que le asisten.

f. La circunstancia de que los datos proporcionados vayan a formar parte de un registro o banco de datos de acceso público.

Por otra parte, la propuesta busca garantizar que también en los actos de recogida de datos desde terceros, es decir, no directamente del titular, se informe debidamente al titular de los datos de forma expresa, precisa, clara e inequívoca.

También se amplía el derecho en cuestión al permitir al titular solicitar información sobre sus datos, al Registro Único Nacional de Banco de Datos.

Por último, se amplía del derecho a exigir información al responsable de la base de datos, respecto de las evaluaciones y evaluaciones que sobre sus datos personales hayan sido comunicadas en los últimos seis meses, así como los criterios empleados para tal evaluación y sus destinatarios.

6. Autorización debe ser expresa.

Enseguida, el proyecto perfecciona el principio de la ley actual que exige el consentimiento del titular para efectuar tratamiento de datos personales, el cual debe efectuarse expresamente y por escrito. Se mantiene dicho principio; pero se señala que sólo tratándose de datos sensibles, la misma deberá otorgarse, además, por escrito.

Se agrega, en todo caso, que aún cuando no se requiera la autorización del titular, deberá informarse a éste conforme a las reglas generales. Se prescinde del consentimiento, mas no del conocimiento del titular.

7. Se regula el flujo transfronterizo de datos.

Por otra parte, el proyecto regula el flujo transfronterizo de datos, exigiendo autorización del Consejo (autoridad controladora) respecto de aquellos países que no cumplan con un nivel de protección adecuado.

8. Se aumentan condiciones de seguridad en el tratamiento de datos.

A continuación, el proyecto establece que el responsable del tratamiento de datos deberá adoptar todas las medidas técnicas y organizativas que garanticen la seguridad de los datos. Además, para fijar las condiciones de seguridad, serán definidas reglamentariamente y no a discreción del responsable del tratamiento de datos, salvo disponga otra cosa un tratado del que Chile sea parte, exista interés público comprometido, o ello sea en interés del propio titular.

9. Se refuerza el deber de rectificación y corrección de datos.

Asimismo, el proyecto hace un cambio en materia de rectificación y corrección de datos. Actualmente, el titular de datos personales tiene derecho a solicitar que estos se modifiquen en caso que sean erróneos, inexactos, equívocos o incompletos. Con la propuesta, se invierte la carga de la prueba respecto de la calidad o corrección de la información, debiendo siempre el responsable de la base de datos modificarlos, a menos que él pruebe que dichos datos son correctos.

Además, se establece que si dichos datos hubieren sido comunicados a terceros, el responsable de la base de datos les deberá informar su corrección o eliminación, estando estos también obligados a rectificar o eliminar los datos en los términos informados.

10. Se regulan infracciones y sanciones.

El proyecto también regula un catálogo pormenorizado de sanciones, en tres niveles, distinguiendo entre sanciones leves, graves y gravísimas, con sus respectivas sanciones, consistentes en multas o cancelación del registro.

Además, regula un procedimiento sancionatorio, que puede iniciarse de oficio o por denuncia. Tal procedimiento garantiza la bilateralidad de la audiencia y el derecho a defensa

del acusado o denunciado. El órgano ante el cual se sigue este procedimiento es el Consejo (autoridad controladora), quien aplicará la sanción. En contra de la resolución que imponga la sanción, se podrá presentar reposición ante el mismo Consejo y en contra de la resolución que se pronuncie sobre esta última, podrá recurrirse de ilegalidad ante la Corte de Apelaciones, en los mismos términos que se regular en el artículo 28 de la Ley de Acceso a la Información Pública.

11. Se perfecciona el sistema de responsabilidad civil.

Además, el proyecto fortalece el derecho del titular a ser reparado por el responsable de la base de datos, de los daños que sufra como consecuencia del incumplimiento de lo previsto en esta ley.

Para ello, se establece una regla de presunción de responsabilidad a favor del titular de los datos, en los casos en que se acredite infracción a lo dispuesto en la ley, de manera que los responsables de las bases de datos tomen efectivamente todas las medidas necesarias para la seguridad de los datos. Además, se establece la responsabilidad solidaria del responsable del tratamiento de datos personales, autor del daño, y los sujetos respecto los cuales éste sea cesionario de dichos datos.

12. Se crea un registro.

Finalmente, el proyecto crea un registro a cargo de el Consejo. Este registro será de carácter público, y en él constará, respecto de cada banco de datos, su responsable, el fundamento jurídico de su existencia, su finalidad, su domicilio, tipos de datos almacenados, descripción del universo de personas que comprende, y destinatarios de los datos personales. Las particularidades de este registro y las normas sobre su implementación serán fijadas reglamentariamente por el Ministerio Secretaría General de la Presidencia.

El responsable del banco de datos proporcionará los antecedentes señalados en el inciso

anterior previo al inicio de sus actividades, y comunicará cualquier cambio que se produzca en ellos dentro de los quince días desde que se verifique.

VI. PRECISIÓN FINAL.

El presente proyecto de ley no establece normas relativas a los datos actualmente regulados en el Título III de la ley N° 19.628. No porque no estime necesaria su modificación y su adecuación a los estándares internacionales sobre la materia, sino porque se ha estimado, que por la especialidad de la materia, es conveniente tratarlo en una ley diferente.

En efecto, en forma paralela a este proyecto, se trabaja en un proyecto para regular el tratamiento de datos sobre obligaciones económicas.

Sin perjuicio de ello, a tales datos, en lo no previsto por su normativa específica, les serán aplicables las normas que acá se establecen sobre protección y los responsables de su tratamiento se encontrarán sometidos a la autoridad del Consejo.

P R O Y E C T O D E L E Y:

“Artículo 1º.- Modifícase la ley 19.628 de la siguiente manera:

1) En el artículo 1°, agrégase el siguiente inciso segundo, nuevo, pasando el actual segundo a ser tercero:

“Toda persona tiene derecho a controlar la información que le concierne, de modo de obtener un adecuado resguardo a sus derechos fundamentales, sin que ello obstaculice innecesariamente el libre flujo de los datos personales.”.

2) En el artículo 2:

a) Sustitúyese en letra i), la expresión “de acceso no restringido o reservado a los solicitantes.”, por las siguientes:

“cuyo acceso no se haya restringido o reservado sólo a los titulares e interesados en los datos personales que contiene, y que no hayan sido calificado como reservados o secretos en la normativa específica que les rija, tales como, la estadística de los censos; los listados telefónicos en los términos previstos por su normativa específica; las listas de personas pertenecientes a grupos de profesionales que voluntariamente se hayan incorporado, consintiendo en el tratamiento público de sus datos, y que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, domicilio o residencia e indicación de su pertenencia al grupo; los diarios y boletines oficiales; y los medios de comunicación social.

El responsable del banco de datos deberá arbitrar las medidas necesarias para la correcta identificación por los titulares de datos, de la condición de fuente accesible al público.”.

b) Agréganse las siguientes letras finales, nuevas:

“p) Encargado de tratamiento, la persona física o jurídica, autoridad pública, servicio o cualquier tercero que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

q) El Consejo, el Consejo para la Transparencia y Protección de Datos Personales.”.

3) En el artículo 3, reemplázase, en el inciso primero, el punto final (.) por una coma (,), y a continuación, agrégase la siguiente expresión:

“Las consecuencias jurídicas de su negativa, la finalidad para la cual se está solicitando la información, los destinatarios de los datos y la posibilidad de que éstos sean comunicados a terceros.”.

4) Intercálase, entre el artículo 3 y el artículo 4, el siguiente artículo 3 bis, nuevo:

“Artículo 3 bis.- En toda solicitud de datos personales deberá informarse previamente a su titular de modo expreso, preciso, claro e inequívoco:

a) De la existencia de un Registro o banco de datos personales en el cual se consignará la información,

identidad del titular del banco de datos y su domicilio, la finalidad de la recogida de datos y los destinatarios de la información.

b) Del carácter obligatorio o facultativo de la entrega de datos personales que se le soliciten y las consecuencias de la entrega de los datos o de la negativa a suministrarlos.

c) De los derechos que le asisten en virtud de la ley, especialmente el derecho de acceso, rectificación, cancelación y bloqueo.

d) El derecho a revocar su autorización para el tratamiento de los datos que le conciernen y las consecuencias de la revocación.

e) Una dirección física o electrónica válida en la cual pueda ejercer los derechos que le asisten.

f) La circunstancia de que los datos proporcionados vayan a formar parte de un registro o banco de datos de acceso público.

En los actos de recogida electrónica de datos personales deberá implementarse sistemas de advertencia que aseguren el conocimiento por el titular de datos de las condiciones precedentes.

En los actos de recogida de datos desde terceros, deberá informarse al titular de datos de forma expresa, precisa, clara e inequívoca, por el responsable de la base de datos o su representante, dentro de los tres meses siguientes al momento del registro de los datos, de los datos objeto de tratamiento, la procedencia de los datos, así como de lo previsto en las letras a), c), d) y e) del inciso 1° del presente artículo.

Lo previsto en los incisos precedentes no se aplicará en los casos en que la ley expresamente exima a un tratamiento del deber de información, cuando se realice tratamiento de datos con fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible.

Tratándose de comunicaciones comerciales de respuesta directa, en cada comunicación que se dirija al titular de datos se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten.”.

5) En el artículo 4:

a) Remplázase el actual inciso tercero, por el siguiente:

"La autorización deberá ser expresa, y tratándose de datos sensibles deberá otorgarse, además, por escrito, manual o electrónicamente.".

b) Suprímese, en el inciso cuarto, la palabra "también".

c) Suprímese, en el inciso quinto, la expresión final:

", o sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios".

d) Remplázase el inciso final, por siguiente nuevo:

"En todo caso, quienes realicen tratamiento de datos personales sin autorización del titular conforme a las disposiciones de este artículo, deberán informar del tratamiento al titular de datos, en los términos del artículo 3 bis.".

6) Elimínanse los incisos quinto y sexto del artículo 5º.

7) Intercálase, entre el artículo 5 y el artículo 6, el siguiente artículo 5 bis, nuevo:

"Artículo 5 bis. No podrán realizarse transferencias de datos personales a países que no proporcionen un nivel de protección adecuado, conforme a la presente ley, salvo autorización previa del Consejo, la que sólo podrá otorgarse si se obtienen garantías adecuadas.

La adecuación del nivel de protección proporcionado por el país de destino será evaluada a la luz de las circunstancias que rodeen a la transferencia. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y duración del tratamiento, el país de origen, el país de destino y las reglas relativas al tratamiento que existan en ese país.

Se exceptúan de la prohibición prevista en el inciso primero, la transferencia consentida por el titular de datos, y los casos en que ésta fuere necesaria para la ejecución de un contrato entre el interesado y el responsable del registro o base de datos; para la aplicación de medidas precontractuales adoptadas a petición del interesado; para la celebración o

ejecución de un contrato entre el responsable del registro o banco de datos y un tercero en interés del interesado; para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial; o para la protección del interés vital del interesado.

Queda asimismo exceptuada la transferencia internacional de datos personales que resulte de la aplicación de tratados o convenios internacionales en los que el Estado de Chile sea parte, o bien cuando la transferencia fuere necesaria o legalmente exigida para salvaguardar un interés público o cuando se haga a efectos de prestar o solicitar auxilio judicial internacional.”.

8) En el artículo 7, agrégase, a continuación de la expresión “que trabajan en el tratamiento de datos personales”, la siguiente expresión:

“o tengan acceso a estos de otra forma”.

9) En el artículo 9, remplázase, a continuación de la expresión “fuentes accesibles al público”, el punto (.), por una coma (,), y a continuación, agrégase la siguiente expresión:

“en los casos mencionados en el artículo 4 precedente.”.

10) En el artículo 10, agrégase el siguiente inciso segundo, nuevo:

“En todo caso los datos personales que se almacenen en virtud del inciso anterior deberán ser los indispensables para el cumplimiento de los fines para los que fueron recolectados y mantenerse por el tiempo estrictamente necesario para el cumplimiento de los fines que motivaron la recolección.”.

11) En el artículo 11, agréganse los siguientes incisos tercero, cuarto y quinto, nuevos:

“El responsable del tratamiento de datos deberá arbitrar las medidas técnicas y organizativas que garanticen la seguridad de los datos de carácter personal y eviten su tratamiento indebido.

Reglamentariamente serán fijadas las condiciones de seguridad que deben adoptarse por el responsable del tratamiento a efectos de dar cumplimiento a las obligaciones a que se refiere el presente artículo.

Se considerará indebido el registro de datos de carácter personal en registros o bancos de datos que no den

cumplimiento a las exigencias que determine el reglamento a que se refiere el presente artículo.”.

12) En el artículo 12:

a) Agrégase el siguiente inciso primero nuevo:

“Toda persona podrá solicitar al Registro Único Nacional de Bancos de Datos información sobre la existencia de tratamientos de datos de carácter personal que pudieren afectarle, sus finalidades y todos los antecedentes necesarios para la identificación del responsable del tratamiento. El Registro Único será de consulta pública y gratuita.”.

b) Agrégase al actual inciso primero, a continuación de la palabra “regularmente”, y antes del punto (.), la siguiente expresión:

“y las evaluaciones y apreciaciones que sobre dicha información hayan sido comunicadas durante los últimos seis meses, así como los criterios de apreciación empleados, el nombre y dirección de la persona o entidad a quien se hayan comunicado los datos”.

c) Agrégase, al actual inciso segundo, a continuación de la palabra “modifiquen”, y antes del punto (.), la siguiente expresión:

“salvo que el responsable del registro o banco de datos acredite lo contrario”.

d) Agrégase, al actual inciso quinto, a continuación de la expresión “podrá ejercerse personalmente” y antes del punto (.), la siguiente expresión:

“o debidamente representado”

13) Remplázase el artículo 16 por el siguiente:

“Artículo 16.- La solicitud a que se refiere el inciso segundo del artículo 12 de esta ley, debe ser ejercida ante el responsable del banco de datos.

Si éste no se pronunciare sobre la solicitud del requirente dentro de diez días hábiles siguientes, o veinte días hábiles tratándose de órganos de la administración del Estado, o la denegare injustificadamente, o tratándose de un órgano público no se encuentre amparado por la deberes de reserva derivados de la seguridad nacional, el titular de los datos

tendrá derecho a recurrir ante el Consejo. Dicha reclamación se regirá por el procedimiento previsto en título V de esta ley.”.

14) En el artículo 19, elimínase, a continuación de la expresión “a fin de que consigne el nuevo dato que corresponda”, la expresión “, previo pago de la tarifa si fuere procedente, con cargo al deudor”.

15) En el artículo 21, agrégase el siguiente inciso primero nuevo, pasando los actuales primero y segundo, a ser segundo y tercero:

“La información relativa a sanciones administrativas o penales sólo podrá ser tratada por organismos públicos, y dentro del marco de su competencia.”.

16) Remplázase el artículo 22 por el siguiente:

“Artículo 22.- Los registros o bancos de datos de titularidad pública deberán inscribirse en el Registro Único Nacional de Bases de Datos.

El organismo público responsable del banco de datos proporcionará esos antecedentes al Registro previo al inicio de las actividades del banco, y comunicará cualquier cambio dentro de los quince días desde que se produzca.”.

17) Remplázase el artículo 23, por el siguiente:

“Artículo 23.- Las infracciones a las disposiciones de esta ley se calificarán como leves, graves y gravísimas.

Son infracciones leves:

a) No entregar oportunamente satisfacción a una solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda.

b) No entregar oportunamente la información solicitada por el Consejo en el ejercicio de sus funciones.

c) Infringir el deber de registro del Banco de Datos, cuando no sea constitutivo de infracción grave.

d) Infringir el deber de información en la recogida de datos personales, cuando no sea constitutivo de infracción grave o gravísima.

Son infracciones graves:

a) Realizar tratamientos de datos personales para finalidades distintas de la motivó su recogida.

b) Realizar tratamiento de datos personales sin consentimiento expreso del titular, en los casos en que éste sea exigible.

c) Realizar tratamiento de datos personales con infracción a los principios y garantías establecidos en la presente ley o su reglamento, cuando no constituya infracción gravísima.

d) Impedir u obstaculizar el ejercicio de los derechos de acceso y oposición.

e) Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan.

f) Vulnerar el deber de secreto y confidencialidad en el tratamiento de datos, establecido en la ley, cuando no se trate de una infracción gravísima.

g) No guardar la debida diligencia en el establecimiento de medidas de seguridad del tratamiento de datos personales.

h) No entregar la información solicitada por el Consejo en el ejercicio de sus funciones.

i) Obstruir de cualquier forma el ejercicio de las atribuciones de inspección del Consejo.

j) No inscribir el registro o banco de datos personales en el Registro Único Nacional de Bases de Datos, habiendo sido requerido para ello por el Consejo.

k) Infringir el deber de información al titular de los datos.

Son infracciones gravísimas:

a) Recoger fraudulentamente datos personales.

b) Comunicar o ceder los datos de carácter personal, fuera de los casos previstos en la ley.

c) Realizar operaciones de tratamiento de datos sensibles fuera de los casos previstos en la ley.

d) Incumplir las instrucciones impartidas por el Consejo sobre las condiciones de legitimidad de un tratamiento de datos.

e) Realizar tratamiento de datos personales de forma ilegítima o con menosprecio de los principios y garantías que establece la ley, cuando de ello derive afectación a derechos fundamentales del titular de datos personales.

g) Vulnerar el deber de guardar secreto sobre los datos sensibles, y datos relativos a sanciones penales y/o administrativas.

h) No atender, u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.

i) No atender de forma sistemática el deber legal de información de la inclusión de datos de carácter personal en un registro o banco de datos.”.

18) Agrégase el siguiente artículo 24, nuevo:

“Artículo 24.- Las infracciones cometidas por particulares serán sancionadas de la siguiente forma:

a) Las infracciones leves serán sancionadas con multa de hasta 200 UTM.

b) Las infracciones graves serán sancionadas con multa de hasta 5000 UTM.

c) Las infracciones muy graves serán sancionadas con multa de hasta 10.000 UTM. El Consejo además podrá disponer la cancelación del registro.

El monto específico de las multas se determinará apreciando fundadamente la gravedad, las consecuencias del hecho, el volumen de los tratamientos efectuados, la capacidad económica del infractor y si éste hubiere cometido otras infracciones de cualquier naturaleza en los últimos 24 meses. La reparación otorgada por el infractor al afectado, previo acuerdo entre ambos, será considerada como una atenuante.

En caso que se verifique la concurrencia de dos o más infracciones subsumibles, se aplicará la sanción correspondiente a la infracción más grave. En los demás casos, se acumularán las sanciones correspondientes a las infracciones concurrentes.

En caso de tratarse de infracciones reiteradas de la misma naturaleza, podrá aplicarse una multa hasta de 3 veces del valor máximo contemplado.

El monto de las multas será a beneficio fiscal y deberá ser pagado en la Tesorería General de la República dentro del plazo de 10 días, contados desde la notificación de la resolución que condena a su pago.”.

19) Agrégase el siguiente artículo 25, nuevo:

“Artículo 25.- Las infracciones leves prescribirán en el plazo de un año, las graves en dos años y las gravísimas en tres años.

Los plazos establecidos en el inciso anterior se contarán desde el día de comisión de la infracción.”.

20) Agrégase el siguiente artículo 26, nuevo:

“Artículo 26.- El procedimiento administrativo para la aplicación de las sanciones previstas en esta ley, se sujetará a las siguientes reglas:

1) Podrán iniciarse de oficio por el Consejo o por denuncia presentada ante él. El Consejo, en ambos casos, impulsará de oficio el procedimiento, haciendo expeditos los trámites que deba cumplir el expediente y removiendo todo obstáculo que pueda afectar a su pronta y debida precisión.

2) La instrucción de oficio del procedimiento se iniciará con una formulación precisa de los cargos, que se notificará al presunto infractor por carta certificada en el domicilio que conste en el Registro Único Nacional de Bases de Datos.

La formulación de cargos señalará una descripción de los hechos que se estimen constitutivos de infracción y la fecha de su verificación, la norma eventualmente infringida y la disposición que establece la infracción, la sanción asignada y el plazo para formular descargos.

3) La denuncia que dé inicio a un procedimiento se formulará por escrito al Consejo, señalando lugar y fecha de presentación y la individualización completa del denunciante, quien deberá suscribirla personalmente o por su mandatario o representante habilitado. Asimismo, deberá contener una descripción de los hechos concretos que se estiman constitutivos de infracción, precisando lugar y fecha de su comisión y, de ser posible, identificando al presunto infractor.

Sin embargo, la denuncia originará un procedimiento sancionatorio sólo si a juicio del Consejo está revestida de seriedad y tiene mérito suficiente. En caso contrario, se podrá disponer la realización de acciones de fiscalización sobre el presunto infractor y si ni siquiera

existiere mérito para ello, se ordenará el archivo de la misma por resolución fundada, notificando de ello al interesado.

Declarada admisible, la denuncia será puesta en conocimiento del presunto infractor.

4) Iniciado el procedimiento, el Consejo dictará una resolución estableciendo las medidas que se deban adoptar para el cese de los efectos de la infracción, la que será notificada al responsable del registro o banco de datos y a los afectados si los hubiere.

5) Las notificaciones se harán por escrito mediante carta certificada dirigida al domicilio del presunto infractor que conste en el Registro Único Nacional de Bases de Datos.

6) El acusado o denunciado tendrá un plazo de diez días hábiles, contados desde la notificación, para contestar los cargos o la denuncia.

7) Recibidos los descargos o transcurrido el plazo otorgado para ello, el Consejo resolverá de plano cuando pueda fundar su decisión en hechos que consten en el proceso o sean de pública notoriedad. En caso contrario, abrirá un término de prueba de ocho días. Dicho plazo se ampliará en caso que corresponda de acuerdo a los artículos 258 y 259 del Código de Procedimiento Civil.

El Consejo dará lugar a las medidas o diligencias probatorias que solicite el presunto infractor en sus descargos, siempre que resulten pertinentes y conducentes. En caso contrario, las rechazará mediante resolución motivada.

8) Los hechos investigados y las responsabilidades de los infractores podrán acreditarse mediante cualquier medio de prueba admisible en derecho, los que se apreciarán en conciencia.

9) La resolución que ponga fin al procedimiento sancionatorio será fundada y resolverá todas las cuestiones planteadas en el expediente, pronunciándose sobre cada una de las alegaciones y defensas del acusado y contendrá la declaración de la sanción que se imponga al infractor o su absolución.

Esta resolución deberá dictarse dentro de los diez días siguientes a aquél en que se haya evacuado la última diligencia ordenada en el expediente.

10) En contra de la resolución referida en el número anterior, se podrá presentar recurso de reposición ante el

Consejo dentro de los cinco días siguientes a su notificación, haciendo valer todos los antecedentes de hecho y de derecho que fundamenten su reclamo. El Consejo deberá resolver dicho recurso dentro de los diez días siguientes de expirado el plazo para interponerla, quedando en suspenso, mientras tanto, el pago efectivo de la multa.

11) En contra la resolución del Consejo que se pronuncie sobre la reposición interpuesta conforme al número anterior, podrá deducirse ilegalidad regulada en el artículo 28 de la ley sobre acceso a la información pública.”.

21) Agrégase el siguiente artículo 27, nuevo:

“Artículo 27.- Los afectados como consecuencia del incumplimiento de lo previsto en la presente ley, tendrán derecho a ser indemnizados por el responsable del banco de datos.

Serán solidariamente responsables, para estos efectos, los responsables del tratamiento de datos, y quienes respecto de los cuales estos sean cesionarios de dichos datos.

Se presumirá legalmente la responsabilidad del autor del daño, si existe infracción a las normas de esta ley.”.

22) Agrégase el siguiente artículo 28, nuevo:

“Artículo 28.- Será competente para conocer de la acción a que se refiere el artículo anterior, el juez de letras del domicilio del demandado o del afectado, a elección de este último.

El procedimiento se regirá de acuerdo a las reglas del procedimiento sumario.”.

Artículo 2º.- Introdúcense las siguientes modificaciones a la ley Nº 20.285:

1) Al artículo 1°:

a) Agrégase el siguiente nuevo inciso segundo, pasando el actual segundo a ser tercero:

“Asimismo, tiene por objeto velar por el adecuado cumplimiento de la normativa sobre protección de datos personales, por parte de organismos públicos y personas naturales, o jurídicas de carácter privado, junto con establecer un sistema único nacional de registro de los bancos de datos personales.”.

b) Agrégase, en el numeral dos del actual inciso segundo, entre la palabra “Transparencia” y el punto aparte, la expresión “y Protección de Datos Personales”.

2) Al artículo 2º, agrégase el siguiente inciso final, nuevo:

“El inciso segundo del artículo anterior, también será aplicable a todos los organismos públicos y personas naturales, o jurídicas de carácter privado, que efectúen las actividades señaladas en el primer inciso del artículo 1° de la ley Nº 19.628.”.

3) En el artículo 7º, agrégase, en el inciso primero, a continuación de la letra m), la siguiente letra n), nueva:

“n) La circunstancia de ser responsables de registros o bancos de datos de carácter personal.”.

4) Modifícase la denominación del Título V, por la siguiente:

“EL CONSEJO PARA LA TRANSPARENCIA Y PROTECCIÓN DE DATOS PERSONALES”.

5) En el artículo 32, agrégase, el siguiente inciso segundo, nuevo:

“Además, el Consejo tendrá por objeto velar por el adecuado cumplimiento de la normativa sobre tratamiento y protección de datos personales, a nivel nacional y conforme a la ley.”.

6) En el artículo 33:

a) Intercálase, en el enunciado del inciso primero, después de la coma que sigue a la expresión “un consejo” y la palabra “tendrá”, la siguiente expresión:

“en razón de lo señalado en el inciso primero del artículo anterior, “.

b) Elimínase la letra m).

7) Intercálase entre el artículo 33 y el artículo 34, el siguiente artículo 33 bis nuevo:

"Artículo 33 bis.- En razón de lo señalado en el inciso segundo del artículo 32, el Consejo tendrá las siguientes funciones y atribuciones:

a) Mantener un Registro Único Nacional de las Bases de Datos, sean estas de origen público o privado, en adelante, el Registro.

Este registro tendrá carácter público, y en él constará, respecto de cada banco de datos, su responsable, el fundamento jurídico de su existencia, su finalidad, su domicilio, los tipos de datos almacenados, la descripción del universo de personas que comprende, y los destinatarios de los datos personales. Las particularidades de este registro y las normas sobre su implementación, serán establecidas por decreto supremo reglamentario del Ministerio Secretaría General de la Presidencia.

El responsable del banco de datos proporcionará los antecedentes señalados en el inciso anterior previo al inicio de sus actividades, y comunicará cualquier cambio que se produzca en ellos dentro de los quince días desde que se verifique.

El Consejo podrá disponer la simplificación o la omisión del registro, cuando se tratare de categorías de tratamientos que no afecten a los derechos y libertades de los interesados, habida cuenta de los datos a que se refieren, y cuando el tratamiento se efectúe en el cumplimiento de disposiciones legales o reglamentarias.

Tratándose del tratamiento de datos personales sensibles, el Consejo determinará cuales de ellos deban ser examinados previamente a entrar en funciones.

b) Fiscalizar el cumplimiento de las normas sobre tratamiento y protección de datos personales, respecto de las bases de datos, públicas y privadas. Para ello, podrá recabar, en cualquier momento, del responsable del respectivo registro o banco de datos, la información que estime pertinente, la que deberá ser remitida en un plazo de diez días, contados desde la fecha de la solicitud. Tratándose de órganos públicos el plazo será de 20 días.

Junto con lo anterior, podrá inspeccionar los registros o bancos de datos personales a efectos de verificar el cumplimiento de las obligaciones que establece la ley. Esta facultad podrá ejercerse tanto respecto a la verificación de las condiciones de seguridad física como en relación al funcionamiento de sistemas informáticos utilizados para el tratamiento de los datos. En todo caso, los funcionarios que ejerzan la inspección a que se refiere esta disposición estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de estas funciones, incluso después de haber cesado en las mismas.

Los responsables de registros o bancos de datos deberán proveer todas las facilidades necesarias para el ejercicio de esta atribución por parte de la autoridad competente. La negativa u obstrucción al ejercicio de esta atribución será considerada una infracción gravísima.

Para el ejercicio de esta facultad, el Consejo podrá requerir el auxilio de la fuerza pública.

c) Requerir la inscripción de los bancos de datos que no estén registrados, en el Registro Único Nacional.

d) Dictar instrucciones de carácter general o particular, respecto de las condiciones de legitimidad de un tratamiento de datos.

e) Conocer de las reclamaciones de particulares relacionadas con el ejercicio de sus derechos, en materia de tratamiento y protección de datos personales, sin perjuicio de las facultades de otras autoridades públicas.

f) Sancionar a los responsables de los bancos de datos que infrinjan las normas sobre tratamiento y protección de datos personales.

g) Requerir a los responsables y encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos al ordenamiento jurídico y, en su caso, ordenar la cesación de los tratamientos y cancelación del registro, cuando no se ajuste a dichas disposiciones.

h) Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal y promover el respeto de los mismos.

j) Ejercer el control y adoptar las autorizaciones que procedan para las transferencias internacionales de datos, conforme lo establecido en la ley N° 19.628; así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales.

k) Entregar una cuenta anual sobre la actividad desarrollada en torno a la protección de datos personales.”.

8) Intercálase entre el artículo 47 y el artículo 48, el siguiente artículo 47 bis, nuevo:

“Artículo 47 bis.- La autoridad o jefatura o jefe superior del órgano o servicio de la Administración del Estado que infrinja lo dispuesto en la normativa sobre

tratamiento y protección de datos, será sancionado con la suspensión en el cargo, por un lapso de cinco a quince días, y/o con multa de 20 a 50% de su remuneración. En la determinación de estas sanciones, se considerará si la infracción ha sido leve, grave o gravísima.

Las sanciones que el Consejo imponga a personas naturales, o jurídicas de carácter privado, responsables de bancos de datos personales, serán las señaladas en el artículo 24 de la ley N° 19.628 y en otras normas sobre protección de datos de carácter personal.”.

9) Ene el artículo 49, intercálase, en el inciso primero, entre las palabras “sanciones” y “previstas”, la siguiente expresión:

“a entidades públicas”.

10) Agrégase el siguiente inciso segundo, nuevo:

“Las sanciones que el Consejo imponga a las personas naturales, o jurídicas de carácter privado responsables de bancos de datos personales, se aplicarán conforme al procedimiento señalado en el Título V de la ley N° 19.628.”.

Artículo 3º.- La presente ley entrará en vigencia tres meses después de publicada en el Diario Oficial.”.

Dios guarde a V.E.,

MICHELLE BACHELET JERIA
Presidenta de la República

JOSÉ ANTONIO VIERA-GALLO QUESNEY
Ministro
Secretario General de la Presidencia

RENÉ CORTÁZAR SANZ
Ministro de Transportes
y Telecomunicaciones

HUGO LAVADOS MONTES
Ministro de Economía,
Fomento y Reconstrucción