

Proyecto de ley, iniciado en moción de los Honorables Senadores señores Harboe, Araya, De Urresti, Espina y Larraín, sobre protección de datos personales.

Fundamentos.

1.- Protección de datos personales: un derecho autónomo.

En general, -Claudio Ortiz siguiendo el concepto de Ana Garriga- se entiende por protección de datos personales el estatuto jurídico destinado a definir las condiciones sobre las cuales terceros podrán hacer uso de datos que conciernen a una persona. Ello principalmente porque un mal uso de dichos datos puede afectar su entorno personal, social o profesional desde las esferas públicas de su persona hasta los límites de su intimidad. De esta definición resulta necesario clarificar que la protección de datos no persigue abstraer del conocimiento público la información de una persona, sino dotarla de los medios necesarios para controlar quién, cómo, dónde y con qué motivo conoce cualquier información acerca de su persona, sea ésta calificable como íntima o no, pública o secreta.¹

Es así como el concepto de protección de datos personales ha sido producto de una evolución teórica y conceptual, es así como al decir del Prof. Banda Vergara, el derecho a la intimidad o vida privada ha evolucionado conceptualmente desde las primeras proclamaciones derivadas de la revolución burguesa, transitando desde una prerrogativa de corte marcadamente individualista, ligado al derecho de propiedad, pasando por el right of privacy anglosajón, o derecho a estar solo, considerando a la persona no como ente aislado, sino dentro de un contexto social, que es donde adquiere sentido exigir respeto por la intimidad.² En efecto, éste es el cambio de paradigma que ha dado paso a la elaboración conceptual - y su posterior consagración - a un derecho ligado a la privacidad, que reconoce su origen en él, pero que con el paso del tiempo se ha ido nutriendo y dando forma a un derecho diferentes, dotado de un contenido distinto de la privacidad. Nos referimos al derecho a la protección de datos personales.

Ahora bien, como una primera aproximación es necesario tratar de delimitar un contenido mínimo del derecho a la protección de datos personales. En efecto, desde el punto de vista doctrinal la protección de los datos personales, es - como se ha dicho- una derivación del derecho a la intimidad debiendo ser reconocido entonces este derecho como un derecho de tercera generación (así lo señalado en la doctrina española el profesor Antonio Pere Licuo, por ejemplo). Con todo, debemos aclarar que si bien el derecho a la protección de datos personales reconoce su origen en el derecho a la intimidad, se trata de un derecho que posee un contenido y características propias e independientes, que los hacen único y claramente distinguible del derecho a la vida privada o la intimidad. En efecto, y tal y como indica el proyecto de ley Boletín 9384-07 que consagra constitucionalmente el derecho a la protección de datos personales³ se trata de un derecho constitucional autónomo, que si bien reconoce su origen en el derecho a la intimidad, está dotado de un contenido

diferente. A mayor abundamiento la Sentencia 292/2000 de 30 de Noviembre del Tribunal Constitucional Español, da una argumento explícito y claro de por qué este derecho merece una consagración expresa separada del derecho a la intimidad o vida privada, en efecto, el fallo en su considerando 6 indica que: "el derecho fundamenta la protección de datos posee una segunda peculiaridad que lo distingue de otros, como el derecho a la intimidad personal y familiar del art. 18.1 CE. Dicha peculiaridad radica en su contenido, ya que a diferencia de este último, que confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido (SSTC 73/1982, de 2 de diciembre, FJ5; 110/1984, de 26 de noviembre, FJ3; 89/1987, de 3 de junio, FJ3; 231/1988, de 2 de diciembre, FJ3; 197/1991, de 17 de octubre, FJ3, y en general las SSTC 134/1999, de 15 de julio, 144/1999, de 22 de Julio, y 115/2000, de 10 de mayo), el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos, el derecho a acceder, rectificar y cancelar dichos datos.⁴

Se trata entonces de asumir una realidad, y es que en la actualidad el debate sobre la intimidad o privacy no se ubica solamente en el ámbito de una prerrogativa del ser humano. No atañe sólo a él individualmente considerado, sino que estas cuestiones han perdido el carácter exclusivamente individual para asumir cada vez más connotaciones públicas y colectivas.⁵ Es por lo anterior, que el tratamiento de datos personales, debe estar concebido para servir a la persona, manteniéndolas como el foco de protección, toda vez que hablamos de un derecho que la doctrina a denominado de tercera generación.

II.- La legislación Chilena en un contexto global.

La globalización y la rápida evolución tecnológica han planteado nuevos retos que no han sido eficazmente asumidos por nuestro país. En efecto, el ingreso de Chile a OCDE en 2010 significó el compromiso de adecuaciones normativas y modificación de marcos legales, entre ellos el de protección de datos, que no se han realizado desde el ingreso de nuestro país a dicha organización, hace ya seis años. La protección de datos resulta indispensable para el desarrollo de una estrategia y agenda digital y para atraer inversión extranjera. Sobre todo, para concebir las múltiples innovaciones tecnológicas con un acento en los derechos humanos.

Desde hace un tiempo la institucionalidad de la protección de datos en el país se ha visto severamente cuestionada, en especial por la falta de certezas sobre tratamiento del flujo de información. En rigor, la ausencia de normas especiales y modernas y de una institucionalidad específica e independiente que sirva para cautelar efectivamente los derechos asociados al tratamiento de datos han significado graves cuestionamientos a personas jurídicas de derecho público y

privado por parte de la sociedad civil, el mundo académico y el periodismo de investigación. Por otra parte han conspirado en contra de una legislación satisfactoria, el hecho de que existan prácticas de algunos agentes del mercado, que afectando los derechos personales de los ciudadanos, no encuentren un contrapeso en una institucionalidad protectora con respuestas efectivas y disuasivas de dichas prácticas. Lo anterior redundando en que en este momento Chile, al ser considerado como un país con un nivel no adecuado de protección en materia de datos personales ha debido someterse al mecanismo de las cláusulas tipo en los respectivos contratos que se suscriben con empresas extranjeras.⁶

Conforme a lo anterior, es de público conocimiento que nuestra actual ley de protección a la vida privada N°19.628, si bien contiene una serie de principios y garantías, estas no están acorde al entorno tecnológico actual ni de acuerdo a las modernas legislaciones en la materia, pues ha puesto en el centro la actividad económica del tratamiento de datos y no a las personas. En resumen, tal y como indica el informe de la Facultad de Ingeniería Industrial de la U. de Chile denominado "Diseño de un modelo organizacional del Consejo para la Transparencia en su función de protección de datos personales" de mayo de 2010, la discusión sobre la protección de datos personales en Chile ha estado marcada por distintos aspectos tanto del cumplimiento del derecho, como de la economía asociada a la materia. En efecto, pese a que la actual legislación (ley N° 19.628) ha establecido una serie de principios en favor de la protección de datos la garantía de autodeterminación de la información, no ha sido capaz de proporcionar una seguridad apropiada a la información personal, quedando muchos de sus artículos como letra muerta, entre otros factores, por la carencia de una institucionalidad a cargo del buen cumplimiento de la normativa.

A nivel comparado, la protección de datos personales ha tenido un desarrollo importante en América Latina a contar del año 2002, con la articulación de la Red Iberoamericana de Protección de Datos. Hoy en día se encuentra reconocida en casi todas las legislaciones de la región y son varios los países que cuentan con una Autoridad de Control con distintos estándares. Los países que muestran un mayor desarrollo normativo en la materia, han basado sus normas en el modelo europeo, con particularidades, partiendo de la base que no existe como en Europa un derecho latinoamericano. Sin perjuicio de esto la mayoría de las leyes en Latinoamérica se han dictado siguiendo las normas de la Unión Europea a efectos de ser considerados países con una legislación adecuada.

Si bien Chile cuenta con una ley del año 1999, siendo pionero en la región, el estándar es insuficiente y actualmente inferior al de sus países vecinos. En efecto, Argentina dicta la Ley N° 25.326 en el 2000, que crea la Dirección Nacional de Protección de Datos Personales, obteniendo posteriormente la declaración de país adecuado conforme al estándar europeo en 2003. Uruguay en 2008, dicta la Ley N° 18.331, que crea la Unidad Reguladora y de Control de Datos Personales, obteniendo la declaración de país adecuado conforme al estándar europeo en la Decisión de la Comisión Europea de 21 de agosto de 2012.

Le siguen en esa línea Perú con la Ley N° 29.733, de 2011; la Ley N° 8.968, de 2011 en Costa Rica; y la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, de 2010, en México, por mencionar algunas.

Con todo, en Chile han existido esfuerzos por mejorar la situación normativa a través de dos proyectos de ley en actual tramitación en el Congreso Nacional, presentados por el Ejecutivo en los años 2008 y 2012 correspondiente a dos gobiernos distintos, los cuales no han tenido avance legislativo sustancial. En ambos textos, la cuestión en torno al diseño y atribuciones de la institucionalidad, esto es una autoridad de control en materia de datos personales, ha sido difícil de articular algún tipo de consenso político en torno al tipo de modelo de institucionalidad y a los recursos que significarían al erario público. Esto evidencia la relegación del tema de parte de algunos actores del gobierno, y el reconocimiento también explícito, de la insuficiencia de las normas actuales de protección de datos, que permiten la vulneración sistemática a los derechos de privacidad, salud, empleo, educación, entre otros.

El tratamiento de datos en Chile pugna con cualquier norma internacional. No existe control sobre la información personal, ni la posibilidad de impugnar los tratamientos indebidos no consentidos y desinformados. Ni menos aún hay normas claras sobre el tratamiento de datos personales comerciales, cuestión que a pesar de los esfuerzos desplegados en leyes como la n° 20575⁷ que establece el principio de finalidad en el tratamiento de datos personales, la institucionalidad aún no está a la altura de los desafíos, problemas y prácticas nocivas que el mercado y las nuevas tecnologías imponen día a día, en resumen nuestro ordenamiento jurídico no contempla requisitos básicos: seguridad, sanciones y el control a través de un ente especializado y autónomo y pugna además con buenas prácticas promovidas por la OCDE.

A mayor abundamiento, la magnitud de la recogida y del intercambio de datos personales también ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas por su parte también difunden un volumen cada vez mayor de información personal. La tecnología ha transformado tanto la economía como la vida social y si bien debe facilitarse la libre circulación de los datos, debe garantizarse un adecuado nivel de protección a los mismos.

Es un hecho que no contamos con una legislación adecuada, esto es una ley que exprese adecuadamente el principio rector en materia de protección de datos: el control. Este control significa poner a las personas en el centro, se traduce en la entrega de herramientas efectivas para el control de la información personal. Estas herramientas de control presentan una doble faz, un conjunto de derechos y una autoridad con facultades competentes a efectos de la prevenir, difundir, investigar, fiscalizar, detectar y sancionar las infracciones a las leyes de protección de datos.

En ese sentido nuestra ley está desactualizada y no fue concebida para proteger derechos de las personas. Es importante una adecuada protección de los datos personales para el ejercicio de los derechos fundamentales en la red y fuera de ella, en entornos en línea y entornos físicos.

A este respecto, son varios los estándares que es posible adoptar, optándose en la presente moción parlamentaria por el más alto de ellos, el Reglamento Europeo de Protección de Datos 679 del 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y que deroga la Directiva 95/46/CE, como referente.

III.- Idea matriz: Establecer un nuevo esquema normativo que se ajuste a los estándares exigidos por las legislaciones más modernas.

La presente moción propone los siguientes avances, en cuanto los organismos que se sujetan a sus normas, públicos y privados en el estándar más alto. El texto se estructura de la siguiente manera:

- Cambia el foco de la actual ley de protección a la vida privada poniendo en el centro a las personas.
- Hace aplicables sus disposiciones a los organismos que traten datos de titulares que residan en Chile, independiente de donde se realice el procesamiento de los datos.
- Mejora el catálogo de definiciones.
- Acota las excepciones al consentimiento respecto del tratamiento con finalidades diversas.
- Especifica el catálogo de principios.
- Mejora el catálogo de derechos.
- Cambia el enfoque del procedimiento judicial, de manera de invertir la carga de la prueba y ordenar la aplicación de multas de manera directa por el tribunal, que pretenden ser disuasivas de eventuales infracciones a la ley, y contempla la presentación de acciones de clase en aquellos casos en que un número determinado de titulares de datos se vean afectados por el incumplimiento de la ley, estableciendo también la reparación tanto material como moral, de acuerdo a elevados estándares en esta sede.
- Incorpora responsabilidades a los roles de responsable, corresponsable y encargado.
- Señala expresamente las obligaciones tan importantes como las relativas a la seguridad de los datos.
- Establece normas claras sobre tratamiento de datos comerciales.
- Aclara algunos aspectos relacionados con el tratamiento de datos realizados por organismos públicos.
- Incorpora un catálogo de infracciones y sanciones.

Sin embargo, dadas las facultades legislativas de los parlamentarios, no es posible abordar en este proyecto de ley cuestiones básicas y fundamentales como la creación de una autoridad de supervisión y control en la materia, que finalmente entregaría a nuestro país el régimen adecuado de protección, mejorando considerablemente la calidad de la protección de los derechos de las personas. En consecuencia, tampoco es posible abordar en este proyecto de manera eficaz las normas relativas a los sistemas de flujo transfronterizo de datos, el cual se justifica en un régimen de estricta supervisión de parte de dicha autoridad. Tampoco la figura del delegado en protección de datos, como ente obligatorio en ciertos contextos de tratamiento de datos, que cumple entre otros,

un rol importante de coordinación entre los sectores que tratan datos y dichas autoridades.

Es justamente este último punto, la autoridad de control y el modelo institucional, en que las autoridades han demostrado una larga deliberación y discusión, 8 años con exactitud, desde la presentación del primer proyecto de ley en 2008, boletín 6120-07.

Mientras no se cuente con una institucionalidad moderna, con un diseño independiente del ciclo político, especializado y con altos estándares técnicos, las personas continuarán sometidas a un régimen de protección de datos difuso, de acciones procesales en tribunales que resultan engorrosas, costosas en materia probatoria y por ende se mantiene un sistema de vulneración de garantías fundamentales, principalmente por aquellos de aquellos que derechos no están reconocidos en el texto actual de la ley.

Hoy no es posible concebir un tratamiento de datos sin seguridad, sin rendición de cuentas, sin transparencia, sin los derechos a la información, sin la observancia del principio de proporcionalidad, entre otros que se consagran en la presente iniciativa. Es por ello que se justifica de todas maneras una reforma en esta materia, de forma de mejorar el estándar de derechos, los principios que la ley establece y las obligaciones de los responsables e impulsar de esa manera los profundos cambios legislativos que son necesarios.

PROYECTO DE LEY SOBRE PROTECCIÓN DE DATOS PERSONALES.

Título I

Disposiciones generales

Artículo 1°

Objeto

La presente ley tiene por objeto asegurar a las personas naturales el derecho a proteger y controlar sus datos personales, de modo de garantizar el ejercicio de sus derechos fundamentales.

El tratamiento de los datos de carácter personal, sean manuales o automatizados, independientemente del medio o soporte en que se encuentren contenidos, se sujetará a las disposiciones de esta ley. Se excluyen los datos personales almacenados en bases de datos domésticas y para actividades relacionadas con su vida privada y familiar. En caso de que pierdan tal carácter quedarán sujetas a esta ley.

El tratamiento de datos personales que se realice en el ejercicio de las libertades de emitir opinión y de informar, se regulará por las leyes a que se refiere el artículo 19 N°12 de la Constitución Política de la República. En todo caso, los medios de comunicación social se regirán por esta ley en lo referido a las bases de datos personales que mantengan para finalidades distintas a las de opinar e informar, tales como las bases de datos de clientes y personal.

Artículo 2°

Ámbito de aplicación territorial

La presente ley se aplica al tratamiento de datos personales en el contexto de las actividades de un responsable o encargado en el territorio nacional, independientemente de que el tratamiento tenga lugar en Chile o no.

Asimismo, se aplica al tratamiento de datos personales cuyos titulares residan en Chile por parte de un responsable o encargado no establecido en Chile, cuando las actividades de tratamiento estén relacionadas con:

- a) la oferta de bienes o servicios a dichos titulares en Chile, independientemente de si a éstos se les requiere su pago, o
- b) el control o seguimiento de su comportamiento, en la medida en que éste tenga lugar en Chile.

Artículo 3°

Definiciones

A efectos de la presente ley se entenderá por:

- 1) Datos personales: toda información sobre una persona natural identificada o identificable. Se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante información combinada con otros datos, en particular mediante un identificador, como el número de cédula de identidad, el análisis de elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;
- 2) Datos sensibles o especialmente protegidos: todo dato personal cuyo tratamiento pueda dar origen a una discriminación arbitraria o ilegal o conlleve un grave riesgo para su titular, tales como, datos de niños y niñas, aquellos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, los datos relativos a la salud, la vida u orientación sexual, los datos genéticos, biométricos, entre otros.
- 3) Tratamiento de datos: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de ellos, ya sea por procedimientos automatizados o no, tales como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, indexación, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;
- 4) Elaboración de perfiles: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona natural, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona, entre otras;
- 5) Procedimiento de disociación de datos: todo tratamiento de datos personales que permita que no puedan atribuirse a un titular, sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona natural identificada o identificable;

- 6) Base de datos: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados.
- 7) Fuente de Acceso Público: base de datos cuyo acceso o consulta puede ser efectuado legítimamente por cualquier persona, sin más exigencia que, en su caso, el pago respectivo como contraprestación, cuando corresponda. Se entenderá que son fuentes de acceso público exclusivamente:
- a) El Censo Nacional de Población y Vivienda del Instituto Nacional de Estadísticas,
 - b) La Encuesta de Caracterización Socioeconómica Nacional del Ministerio de Desarrollo Social,
 - c) Los repertorios telefónicos en los términos previstos en su normativa específica,
 - d) Las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo.
 - e) Los diarios y boletines oficiales.
 - f) Los medios de comunicación.
- 8) Titular: la persona a la que se refieren los datos de carácter personal
- 9) Responsable del tratamiento o responsable: la persona natural o jurídica que, solo o junto con otros, determine los fines y medios del tratamiento;
- 10) Encargado del tratamiento o encargado: la persona natural o jurídica que trate datos personales por cuenta del responsable del tratamiento;
- 11) Intermediarios en el tratamiento: persona natural o jurídica, distinta del responsable y del encargado, que presta servicios de infraestructura, plataforma, software u otros servicios a los responsables y/o encargados para el almacenamiento de los datos personales tratados y/o para facilitar enlaces a éstos o instrumentos de búsqueda, sin que ello importe realizar operaciones de tratamiento sobre los referidos datos. Los intermediarios estarán sujetos a los mismos deberes, responsabilidades y sanciones que los encargados.
- 12) Destinatario: la persona natural o jurídica al que se comuniquen datos personales, se trate o no de un tercero.
- 13) Tercero: persona natural o jurídica distinto del titular, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo el dominio directo del responsable o del encargado;
- 14) Consentimiento: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el titular acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen;
- 15) Violación de la seguridad de los datos personales: todo incidente de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales tratados o la comunicación o acceso no autorizados a dichos datos;
- 16) Datos genéticos: datos personales relativos a las características genéticas heredadas o adquiridas de una persona natural que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona,
- 17) Datos biométricos: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona natural que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;

18) Datos relativos a la salud: datos personales relativos a la salud física o mental de una persona natural, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud;

19) Organismos Públicos: las autoridades, órganos del Estado y organismos, descritos y regulados por la Constitución Política de la República, y los comprendidos en el inciso segundo del artículo 1° de la ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado.

20) Transferencia internacional de datos: cualquier transmisión de datos personales fuera del territorio nacional, independientemente si el objeto de ésta es una cesión de datos o un tratamiento de los datos por cuenta del responsable de la base de datos.

Artículo 4°

Licitud del tratamiento

El tratamiento de los datos personales sólo puede efectuarse con sujeción a las normas de la presente ley.

El tratamiento sólo será lícito si se cumple, al menos, una de las siguientes condiciones:

- a) El titular haya dado su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
- b) El tratamiento sea necesario para la ejecución de un contrato en el que el titular sea parte o para la aplicación a petición de éste de medidas precontractuales;
- c) el tratamiento sea necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
- d) el tratamiento sea necesario para proteger intereses vitales del titular o de otra persona natural;
- e) los datos personales sean tratados por los órganos del Estado en el ejercicio de sus competencias y en la forma prescrita en la ley;
- f) el tratamiento sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que los datos hubiesen sido obtenidos de una fuente de acceso público, y sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales de los titulares de los datos que requieran la protección de datos personales, en particular cuando los titulares sean niños.

Artículo 5°

Consentimiento

El consentimiento es toda manifestación de voluntad libre, inequívoca, específica e informada, mediante la que el titular autoriza el tratamiento de sus datos personales. La persona que autoriza debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y su posible comunicación o cesión a terceros.

Al evaluar si el consentimiento se ha dado libremente, se tendrá en consideración el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento el

tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato. El consentimiento no constituirá una base jurídica válida para el tratamiento cuando exista un desequilibrio claro entre la posición del titular y el responsable del tratamiento.

El titular puede revocar el consentimiento otorgado, sin efecto retroactivo, en cualquier tiempo, sin expresión de causa y utilizando técnicas o medios similares a aquellos a través de los cuales lo otorgó.

La revocación del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retiro.

Si el consentimiento del titular se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo.

El responsable del tratamiento asumirá la carga de la prueba de que el titular ha dado su consentimiento para el tratamiento de sus datos personales para determinados fines.

No será vinculante ninguna parte de la declaración que constituya una infracción a la presente ley.

Artículo 6º

Tratamiento para un fin distinto que aquél para el que se recogieron los datos personales

Cuando se realice tratamiento de datos con una finalidad distinta de aquella para el que se recogieron los datos personales, con objeto de determinar si el tratamiento con otro fin es compatible y lícito, se tendrá en cuenta, entre otras cosas:

- a) Cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento posterior previsto;
- b) El contexto en que se hayan recogido los datos personales, en particular en lo que respecta a la relación entre los titulares y el responsable del tratamiento;
- c) La naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, o datos personales relativos a condenas e infracciones penales.
- d) Las posibles consecuencias para los titulares del tratamiento ulterior previsto;
- e) La existencia de garantías adecuadas, que podrán incluir el cifrado o la disociación de datos.

Artículo 7º

Cesión de datos personales.

Los datos personales sólo podrán ser cedidos con el consentimiento del titular y para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario.

No será necesario el consentimiento erigido en el inciso anterior cuando:

- a) La cesión esté autorizada en una ley;
- b) La cesión derive de una relación contractual del titular de los datos y sea la consecuencia de un contrato, cuyo desarrollo, cumplimiento y control requiera la transferencia de los datos a terceros. En este caso la cesión será legítima en la medida que se limite a la finalidad que le sirve de causa;
- c) La cesión se produzca entre órganos del Estado, en el ejercicio de sus funciones y atribuciones y el tratamiento de los datos tenga fines históricos, estadísticos o científicos;

En caso que el consentimiento otorgado por el titular al momento de la recolección de los datos no haya considerado la cesión de los mismos, deberá informarse al titular antes de ésta se produzca, la finalidad a la cual serán destinados los datos o el tipo de actividad de aquel a quien se le pretenden ceder.

El cesionario de los datos personales queda obligado a esta ley, por el sólo hecho de la cesión y pasará a ser considerado para todos los efectos legales responsable.

Artículo 8°

Principios del tratamiento de datos

El tratamiento de datos personales se someterá a los principios de legitimidad, finalidad, calidad, proporcionalidad, transparencia, responsabilidad y rendición de cuentas, confidencialidad, minimización, temporalidad y seguridad.

- a) Legitimidad: Los datos serán tratados de manera lícita y leal en relación con su titular.
- b) Finalidad: Los datos solo serán tratados con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; el tratamiento posterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales.
- c) Calidad: Los datos personales deben ser adecuados, pertinentes y responder con veracidad a la situación real de la persona titular de los datos. Deberán ser exactos y actualizados, debiendo los responsables adoptar todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.
- d) Proporcionalidad: El tratamiento de datos personales deberá circunscribirse a aquéllos datos que resulten adecuados, necesarios, relevantes y no excesivos en relación con las finalidades previstas en el tratamiento y considerar entre los medios con que pueda llevarse a cabo dicho tratamiento, el menos lesivo para los derechos de los titulares de dichos datos.
- e) Transparencia: El responsable del tratamiento tomará las medidas oportunas para facilitar al titular toda la información que señala esta ley, así como cualquier comunicación relativa al tratamiento, en forma concisa, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos.

f) Responsabilidad y rendición de cuentas: El responsable del tratamiento será responsable del cumplimiento de la presente ley, debiendo ser capaz de demostrarlo.

g) Confidencialidad: Quienes trabajen en el tratamiento de datos personales y el encargado que tenga acceso a los datos personales sólo podrán tratar dichos datos siguiendo instrucciones del responsable, deberán guardar secreto de los mismos, obligación que no cesa por haber terminado sus actividades en ese campo.

h) Minimización de datos: Toda recolección de datos deberá limitarse a lo necesario en relación con los fines para los que serán tratados.

i) Temporalidad: Los datos sólo deberán ser conservados de forma que se permita la identificación de los titulares durante no más tiempo del necesario para los fines del tratamiento. Podrán conservarse los datos personales durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas a fin de proteger los derechos de los titulares.

j) Seguridad: los datos personales deberán ser tratados de tal manera que se garantice una seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.

Artículo 9º

Datos Especialmente Protegidos

Queda prohibido el tratamiento de los datos especialmente protegidos, a menos que concurra alguna de las siguientes circunstancias:

a) El titular haya dado su consentimiento previo y explícito para su tratamiento.

b) El tratamiento sea necesario para el cumplimiento de obligaciones específicas del responsable del tratamiento o para los derechos del titular en el ámbito del diagnóstico médico, laboral, prestación de asistencia sanitaria o de seguridad social.

c) El tratamiento sea necesario para proteger intereses vitales del titular de los datos, en el supuesto de que el titular no esté capacitado, física o jurídicamente, para dar su consentimiento.

d) El tratamiento sea efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los titulares.

e) El tratamiento se refiera a datos personales que el titular haya hecho voluntariamente públicos;

f) El tratamiento sea necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial.

g) El tratamiento sea realizado por un organismo público en el cumplimiento de una obligación legal.

h) El tratamiento sea necesario con fines de archivo en interés público.

Artículo 10

Tratamiento de datos personales de niños

El tratamiento de los datos personales relativos a los niños y niñas se considerará lícito cuando éstos tengan como mínimo 14 años. Si el niño o niña es menor de 14 años, será necesario el consentimiento de los padres o de su representante legal.

Título II

Derechos de los titulares.

Artículo 11

Derechos de los titulares de datos

Esta ley garantiza a los titulares los derechos de información, acceso, rectificación, cancelación, oposición, bloqueo, impugnación de valoraciones personales y portabilidad de sus datos personales. Toda persona tiene derecho a exigir a quien sea responsable del tratamiento de datos, el ejercicio de sus derechos sobre los datos relativos a su persona. Si a los datos personales tienen acceso diversos organismos, el titular puede ejercer sus derechos ante cualquiera de ellos.

Estos derechos no podrán ser limitados por medio de ningún acto o convención y se ejercerán de manera absolutamente gratuitas, debiendo proporcionarse, además, a solicitud del titular, copia de los registros pertinentes. Los responsables podrán establecer canales de comunicación electrónicos para el ejercicio de los derechos de los titulares, los cuales deberán dar respuesta a los requerimientos en los plazos señalados en el artículo 20.

No obstante, lo dispuesto en este Título no podrá solicitarse la cancelación, oposición 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.

Tampoco podrá cancelación, oposición o bloqueo de datos personales almacenados por mandato legal.

Artículo 12

Derecho de información

El responsable del tratamiento tomará las medidas oportunas para facilitar al titular toda información relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos.

La información que se facilite deberá contener al menos:

a) la identidad y los datos de contacto del responsable y de su representante, cuando correspondiere;

- b) los fines del tratamiento a que se destinan los datos personales y el fundamento jurídico del tratamiento;
- c) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;
- d) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al titular, y su rectificación, cancelación u oposición al tratamiento, así como el derecho a la portabilidad de los datos;
- f) el derecho a recurrir ante los tribunales de justicia en caso de que el responsable no responda o deniegue la solicitud realizada por el titular;
- g) la posible cesión o transferencia internacional y su finalidad, cuando corresponda.
- h) la existencia de decisiones automatizadas, incluida la elaboración de perfiles.

Cuando el responsable del tratamiento pretenda el tratamiento posterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al titular, con anterioridad a dicho tratamiento, información sobre ese otro fin y cualquier información adicional que considere pertinente al tenor del artículo 6°.

Los responsables están igualmente obligados a proporcionar información, cuando los datos personales no se hayan obtenido de los titulares, por la vía más expedita posible, en particular sobre la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público.

Lo anterior no será aplicable cuando el titular de los datos ya disponga de la información, o cuando la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.

Artículo 13

Derecho de acceso

Los titulares de datos tienen derecho a conocer gratuitamente los datos tratados por el responsable, así como al origen de los mismos, las finalidades de los correspondientes tratamientos y los destinatarios o las categorías de destinatarios a quienes se cedan o transfieran dichos datos.

Los titulares tendrán derecho a acceder la información en los términos señalados en el artículo anterior.

Artículo 14

Derecho de rectificación

Se garantiza el derecho del titular de obtener del responsable la rectificación de los datos personales que pudieran resultar incompletos, inexactos, innecesarios o excesivos.

Artículo 15

Derecho de cancelación

Las personas tendrán derecho a obtener la cancelación, supresión o eliminación de los datos personales que le conciernan, sin dilación indebida del responsable del tratamiento, cuando concurra alguna de las circunstancias siguientes:

- a) Los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos;
- b) El titular retire el consentimiento en que se basa el tratamiento y éste no se base en otro fundamento jurídico;
- c) Los datos personales hayan sido tratados ilícitamente;
- d) Cuando se pierda la facultad legal para tratarlos.

Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en este artículo a suprimir dichos datos el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el costo de su aplicación, adoptara medidas razonables, incluidas medidas técnicas, con el propósito de informar a los responsables que estén tratando los datos personales de la solicitud del titular de cancelación de cualquier enlace a esos datos personales, cuando hayan sido difundidos en Internet, o cualquier copia o réplica de los mismos.

Artículo 16

Derecho de oposición

Se garantiza el derecho del titular de oponerse al tratamiento de sus datos personales cuando concurra una razón derivada de su situación personal y, especialmente, cuando:

- a) El tratamiento de los datos carezca de fundamento legal;
- b) El dato personal haya caducado;
- c) El titular hubiese revocado su consentimiento para el tratamiento de sus datos personales;
- d) Sus datos personales son utilizados para comunicaciones comerciales o publicitarias y el titular se haya incluido en algún registro, público o privado, de exclusión publicitaria.
- f) Los datos sean usados para la elaboración de perfiles.

Artículo 17

Derechos ante el tratamiento automatizado de datos

Las personas tienen derecho no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente.

El titular podrá impugnar las decisiones que impliquen una valoración de su comportamiento, cuando el único fundamento sea un tratamiento de datos personales que ofrezca una definición de sus características o personalidad.

En este caso, el titular tendrá derecho a obtener información del responsable respecto a los criterios de valoración como sobre el programa utilizado en el tratamiento que sirvió para adoptar la decisión.

Artículo 18

Derecho al bloqueo del tratamiento

El titular tendrá derecho a obtener del responsable del tratamiento el bloqueo del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:

- a) el titular impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos;
- b) el tratamiento sea ilícito y el titular se oponga a la supresión de los datos personales y solicite en su lugar el bloqueo para ejercer sus acciones legales;
- c) el responsable ya no necesite los datos personales para los fines del tratamiento, pero el titular los necesite para la formulación, el ejercicio o la defensa de reclamaciones;

Artículo 19

Derecho a la portabilidad de datos

Los titulares tendrán derecho a la portabilidad de sus datos personales. Podrán solicitar y recibir sus datos en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando:

- a) el tratamiento esté basado en el consentimiento explicitado en un contrato.
- b) el tratamiento se efectúe por medios automatizados.

Al ejercer su derecho a la portabilidad el titular tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.

Título III

Procedimiento de reclamación

Artículo 20

Procedimiento general

Si el responsable del registro o banco de datos no se pronuncie sobre la solicitud del requirente dentro de dos días hábiles, o siendo organismo público, la denegare por una causa distinta de la seguridad de la Nación o el interés nacional, el titular de los datos tendrá derecho a recurrir al juez de letras en lo civil domicilio del titular de los datos personales, según las reglas correspondientes, solicitando amparo a los derechos consagrados en los artículos precedentes, sujetándose el procedimiento a las reglas siguientes:

- a) La reclamación señalará claramente la infracción cometida y los hechos que la configuran. Si el titular lo solicitare, el tribunal deberá mantener reserva de los hechos y pruebas que acompañen al expediente cuando contengan datos personales.
- b) El tribunal dispondrá que la reclamación sea notificada por el medio más expedito posible, inclusive electrónicamente. En igual forma se notificará la sentencia que se dicte.
- c) El responsable deberá presentar sus descargos dentro de quinto día hábil y adjuntar los medios de prueba que acrediten que ha actuado en cumplimiento de la presente ley.
- d) La sentencia definitiva se dictará dentro de tercero día de vencido el plazo a que se refiere la letra anterior, sea que se hayan o no presentado descargos. Si el

tribunal decretó una audiencia de prueba, este plazo correrá una vez vencido el plazo fijado para ésta.

e) Todas las resoluciones, con excepción de la indicada en la letra f) de este inciso, se dictarán en única instancia y se notificarán por el estado diario.

f) La sentencia definitiva será apelable en ambos efectos. El recurso deberá interponerse en el término fatal de cinco días, contado desde la notificación de la parte que lo entabla, deberá contener los fundamentos de hecho y de derecho en que se apoya y las peticiones concretas que se formulan.

g) Deducida la apelación, el tribunal elevará de inmediato los autos a la Corte de Apelaciones respectiva. Recibidos los autos en la Secretaría de la Corte, el Presidente ordenará dar cuenta preferente del recurso, sin esperar la comparecencia de ninguna de las partes.

h) El fallo que se pronuncie sobre la apelación no será susceptible de los recursos de casación.

En caso de que la causal invocada para denegar la solicitud del requirente fuere la seguridad de la Nación o el interés nacional, la reclamación deberá deducirse ante la Corte Suprema, la que solicitará informe de la autoridad de que se trate por la vía que considere más rápida, fijándole plazo al efecto, transcurrido el cual resolverá en cuenta la controversia. De recibirse prueba, se consignará en un cuaderno separado y reservado, que conservará ese carácter aun después de afinada la causa si por sentencia ejecutoriada se denegare la solicitud del requirente.

La sala de la Corte Suprema que conozca la reclamación conforme al inciso anterior, o la sala de la Corte de Apelaciones que conozca la apelación, tratándose del procedimiento establecido en los incisos primero y segundo, si lo estima conveniente o se le solicita con fundamento plausible, podrá ordenar traer los autos en relación para oír a los abogados de las partes, caso en el cual la causa se agregará extraordinariamente a la tabla respectiva de la misma sala. En las reclamaciones por las causales señaladas en el inciso precedente, el Presidente del Tribunal dispondrá que la audiencia no sea pública.

En caso de acogerse la reclamación, la misma sentencia fijará un plazo prudencial para dar cumplimiento a lo resuelto y el tribunal aplicará una multa de conformidad al Título VII de esta ley.

En caso que el infractor sea un organismo público, el tribunal podrá sancionar al jefe del Servicio con la suspensión de su cargo, por un lapso mínimo de 15 días atendiendo la gravedad de la falta.

Artículo 21

Interés colectivo

En caso que se vea afectado el interés colectivo o difuso de los titulares de datos por incumplimiento a cualquiera de las obligaciones establecidas en la presente ley, será aplicable el procedimiento especial para protección del interés colectivo o difuso de los consumidores establecido en el Párrafo 2° del Título IV de la ley N° 19.496, con las siguientes salvedades:

1.- Será competente para conocer de estas demandas el juez de letras correspondiente al domicilio del demandado.

2.- El número de personas afectadas bajo un mismo interés a que se refiere la letra c) del N° 1 del artículo 51 de la ley N° 19.496 no podrá ser inferior a 20 personas.

3.- No regirá lo dispuesto en los artículos 51 N°9, 52 y 53 de la ley N° 19.496.

4.- Las indemnizaciones podrán extenderse al lucro cesante y al daño moral. Tanto éste como la especie y monto de los perjuicios adicionales sufridos individualmente por cada demandante serán determinados de acuerdo a lo establecido en los incisos segundo y tercero del artículo 54 C de la ley N° 19.496. Mientras se sustancia el juicio quedará suspendido el plazo para demandar este daño.

5.- La sentencia definitiva producirá efectos respecto de todas las personas que tengan el mismo interés colectivo. Aquellas personas a quienes les empiece la sentencia definitiva pero que no hayan ejercido la acción podrán acreditar el interés común en conformidad al inciso primero del artículo 54 C de la ley N° 19.496, previo abono de la proporción que les correspondiere en las costas personales y judiciales en que hayan incurrido las personas que ejercieron la acción.

6.- En caso de no ser habido el demandado, se podrá practicar la notificación de la demanda por el medio más expedito posible, inclusive electrónicamente.

7.- Se acumularán al juicio colectivo los juicios individuales que se hubieren iniciado, a menos que en éstos se haya citado a las partes para oír sentencia.

8.- Acogida total o parcialmente la demanda deberán imponerse las costas a la parte demandada y, si son varios los demandados, corresponderá al tribunal determinar la proporción en que deberán pagarlas.

9.- Serán aprobadas por el tribunal las propuestas de conciliación para poner término al proceso formuladas por la parte demandada, siempre que ellas cuenten con la aceptación de los dos tercios de los demandantes, que se ofrezcan garantías razonables del efectivo cumplimiento de las obligaciones que se contraen, si no fueren de ejecución instantánea y que no se contemplen condiciones discriminatorias para alguno de los actores.

10.- En los contratos que se perfeccionen a partir de la publicación de esta ley no será impedimento para demandar colectivamente el que se haya pactado compromiso de arbitraje, el cual quedará sin efecto por el solo hecho de la presentación de la demanda colectiva.

Título IV

Del tratamiento de datos relativos a obligaciones de carácter económico, financiero, bancario o comercial

Artículo 22

Reglas generales

Los responsables de los registros o bancos de datos o quienes efectúen tratamiento de datos personales a fin de determinar la capacidad crediticia de una persona, sólo podrán tratar datos de carácter personal solo para la finalidad prevista en la ley n° 20.575 y obtenidos de los registros y las fuentes accesibles al público establecido al efecto o procedente de informaciones facilitadas por el interesado o con su consentimiento. También podrán tratarse los datos de incumplimiento facilitados por el acreedor o por quien actúe por su cuenta. Quien se dedique al tratamiento de estos datos, notificara a los interesados el

hecho que sus datos están siendo tratados, por la vía más expedita posible dentro del plazo de 15 días.

Los titulares de datos podrán solicitar del responsable del tratamiento las comunicaciones de los datos que este haya hecho en los últimos 12 meses, como sus evaluaciones, indicando el nombre y dirección de la persona o entidad a quien se hayan revelado los datos. El responsable deberá entregar esta información de manera gratuita.

No podrá comunicarse la información relacionada con las deudas contraídas con empresas públicas o privadas que proporcionen servicios de educación, electricidad, salud, transporte, agua, teléfono, internet y gas; tampoco podrán comunicarse las deudas contraídas con concesionarios de autopistas por el uso de su infraestructura.

Las entidades responsables que administren bancos de datos personales no podrán publicar o comunicar la información referida en el presente artículo, en especial los protestos y morosidades contenidas en él, cuando éstas se hayan originado durante el periodo de cesantía que afecte al deudor.

Para estos efectos, la Administradora de Fondos de Cesantía comunicará los datos de sus beneficiarios al Boletín de Informaciones Comerciales sólo mientras subsistan sus beneficios para los efectos de que éste bloquee la información concerniente a tales personas.

Sin embargo, las personas que no estén incorporadas al seguro de cesantía deberán acreditar dicha condición ante el Boletín de Informaciones Comerciales, acompañando el finiquito extendido en forma legal o, si existiese controversia, con el acta de comparecencia ante la Inspección del Trabajo, para los efectos de impetrar este derecho por tres meses renovable hasta por una vez. Para que opere dicha renovación se deberá adjuntar una declaración jurada del deudor en la que manifieste que mantiene su condición de cesante.

El bloqueo de datos será sin costo para el deudor.

No procederá el bloqueo de datos respecto de quienes consignen anotaciones en el sistema de información comercial durante el año anterior a la fecha de término de su relación laboral.

Las entidades responsables de la administración de bancos de datos personales no podrán señalar bajo ninguna circunstancia, signo o caracterización que la persona se encuentra beneficiada por esta ley.

Artículo 23

Comunicación y cancelación

En ningún caso pueden comunicarse los datos a que se refiere el artículo anterior, que se relacionen con una persona identificada o identificable, luego de transcurridos cinco años desde que la respectiva obligación se hizo exigible.

Deberán cancelarse los datos relativos a obligaciones pagadas o extinguidas por cualquier otro modo legal de extinguir las obligaciones sin requerimiento del titular, y se procederá, para todos los efectos legales, como si estos datos no hubieran existido jamás.

Con todo, se comunicará a los tribunales de Justicia la información que requieran con motivo de juicios pendientes.

Artículo 24

Pago o extinción de la obligación.

El pago o la extinción de estas obligaciones por cualquier otro modo producen la caducidad o la pérdida de fundamento legal de los datos respectivos para los efectos del artículo 11 y siguientes, mientras estén pendientes los plazos que establece el artículo precedente.

Al efectuarse el pago o extinguirse la obligación por otro modo en que intervenga directamente el acreedor, éste avisará tal hecho, a más tardar dentro de los siguientes siete días hábiles, al responsable del registro o banco de datos accesible al público que en su oportunidad comunicó el protesto o la morosidad, a fin de que consigne el nuevo dato que corresponda. El responsable del banco de datos deberá efectuar el cambio respectivo en el banco de datos, sin esperar requerimiento, una vez que haya tomado conocimiento del cambio en las circunstancias del titular de los datos, sea informado por el acreedor o por el mismo deudor.

Quienes efectúen el tratamiento de datos personales provenientes o recolectados de la aludida fuente accesible al público deberán modificar los datos en el mismo sentido tan pronto aquélla comunique el pago o la extinción de la obligación, o dentro de los tres días siguientes. Si no les fuera posible, bloquearán los datos del respectivo titular hasta que esté actualizada la información.

La infracción de cualquiera de estas obligaciones se conocerá y sancionará de acuerdo a lo previsto en el artículo 20.

Artículo 25

Sobre el principio de finalidad.

Las disposiciones de la ley 20.575 que establece el principio de finalidad en el tratamiento de datos personales a que se refiere el presente título, se aplicarán supletoriamente y cuanto resulten compatibles a las disposiciones de esta ley.

Título IV

Del responsable y encargado del tratamiento

Artículo 26

Responsabilidad del responsable y del encargado de tratamiento

Los responsables y encargados deberán llevar un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener, a lo menos, la información indicada a continuación:

- a) el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable;
- b) los fines del tratamiento;
- c) una descripción de las categorías de titulares y de las categorías de datos personales;
- d) las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;
- e) en su caso, las transferencias internacionales de datos personales y la documentación de garantías adecuadas;
- f) Los plazos previstos para la cancelación o eliminación de las diferentes categorías de datos;
- g) Una descripción general de las medidas técnicas y organizativas de seguridad.

Las obligaciones anteriores no se aplicarán a ninguna empresa ni organización que emplee a menos de 200 personas salvo que el tratamiento que realice pueda producir un riesgo para los derechos y libertades de los titulares, tales como el tratamiento masivo de datos, los datos tratados en el desarrollo de aplicaciones móviles o el tratamiento de datos especialmente protegidos.

Artículo 27

Corresponsables del tratamiento

Cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento. Los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por la presente ley, en particular en cuanto al ejercicio de los derechos del titular y a sus respectivas obligaciones de suministro de información. Dicho acuerdo podrá designar un punto de contacto para los titulares. Se pondrán a disposición del titular los aspectos esenciales del acuerdo.

Independientemente de los términos del acuerdo los titulares podrán ejercer sus derechos frente a cualquiera de ellos.

Artículo 28

Responsables no establecidos en Chile

Los responsables del tratamiento no residentes en Chile, deberán designar a un representante en Chile, que atienda, junto al responsable o al encargado, o en su lugar, a las consultas de los titulares, sobre todos los asuntos relativos al tratamiento, a fin de garantizar el cumplimiento de lo dispuesto en la presente ley. La designación de un representante, por el responsable o el encargado del tratamiento, se entenderá sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable o encargado.

Artículo 29

Deberes del encargado del tratamiento

Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, éste deberá elegir únicamente a un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos de la presente ley y garantice la protección de los derechos de los titulares.

El encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito específica o general, del responsable. En este último caso, el encargado informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así al responsable la oportunidad de oponerse a dichos cambios. Cuando un encargado del tratamiento recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este otro encargado, mediante contrato, las mismas obligaciones de protección de datos que se señalan a continuación. Si ese otro encargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento en lo que respecta al cumplimiento de las obligaciones del otro encargado.

El tratamiento por el encargado se registrará por un contrato con arreglo a la legislación vigente, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de titulares, y las obligaciones y derechos del responsable. Dicho contrato estipulará, en particular, que el encargado:

- a) tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias internacionales de datos personales, salvo que esté obligado a ello en virtud de la ley; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento;
- b) garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria o contractual;
- c) tomará todas las medidas necesarias de seguridad, asistiendo al responsable, teniendo en cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que éste pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los titulares.
- d) a elección del responsable, cancelará no devolverá todos los datos personales una vez que finalice la prestación de los servicios de tratamiento, y cancelará las copias existentes a menos que se requiera la conservación de los datos personales en virtud de la ley;
- f) pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

El encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe alguna disposición en materia de protección de datos.

Artículo 30

Registro de actividades de tratamiento

Cada encargado y, en su caso, el representante del encargado, llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable, que contenga:

- a) el nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del representante del responsable o del encargado;
- b) las categorías de tratamientos efectuados por cuenta de cada responsable;
- c) en su caso, las transferencias internacionales de datos personales, incluida la identificación del destinatario;

Las obligaciones anteriores, no se aplicarán a ninguna empresa ni organización que emplee a menos de 200 personas, salvo que el tratamiento que realice pueda producir un riesgo para los derechos y libertades de los titulares, tales como tratamiento masivo de datos o aplicaciones móviles o se traten datos especialmente protegidos.

Título V

Seguridad de los datos personales

Artículo 31

Seguridad del tratamiento

Teniendo en cuenta el estado de la técnica, su costo de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas naturales, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, al menos:

- a) la disociación o el cifrado de datos personales;
- b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
- c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
- d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en especial como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

Artículo 32

Notificación ante incidentes de seguridad de datos personales

Los responsables deberán comunicar a los titulares por los medios más expeditos posibles, las violaciones de la seguridad de datos personales en un

lenguaje claro y sencillo, señalando la naturaleza de dicha incidencia y las medidas de protección técnicas y organizativas adoptadas.

Los responsables cuyo rubro se encuentre bajo la supervisión de una Superintendencia, deberán informar a la brevedad a la autoridad correspondiente sobre los incidentes de seguridad de datos personales y las medidas a adoptar para evitar la afectación de los derechos de los titulares.

Artículo 33

Evaluación de impacto

Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, implique un alto riesgo para los derechos y libertades de las personas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación de los riesgos y el posible impacto de las operaciones de tratamiento en la protección de datos personales.

Esta evaluación será obligatoria en caso de:

- a) evaluación sistemática y exhaustiva de aspectos personales de personas naturales que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas naturales o que les afecten significativamente de modo similar;
- b) tratamiento a gran escala de las categorías especiales de datos o de los datos personales relativos a condenas e infracciones.
- c) observación sistemática a gran escala de una zona de acceso público.

La evaluación deberá incluir como mínimo:

- a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;
- b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;
- c) una evaluación de los riesgos para los derechos y libertades de los titulares, y
- d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con la presente ley, teniendo en cuenta los derechos e intereses legítimos de los titulares y de otras personas afectadas.

Título IV

Del tratamiento de datos por los organismos públicos

Artículo 34

Reglas generales

El tratamiento de datos personales por organismos públicos sólo podrá efectuarse con sujeción a la presente ley y respecto a las materias de las competencias explícitamente señaladas en la ley respectiva.

Con ambas condiciones, no necesitará el consentimiento del titular, sin perjuicio de las medidas de transparencia, rendición de cuentas e información que deba adoptar.

Los datos personales tratados por un órgano del Estado no serán comunicados a otros órganos del Estado, salvo que el destinatario de los datos personales tenga competencia legal para tratarlo.

Los órganos del Estado podrán ceder los datos personales que tratan a otros órganos del Estado con el objeto de prestar servicios o conceder beneficios al titular que los solicita, a fin de evitarle realizar trámites adicionales para recolectar los datos personales, en la medida que se encuentren en poder de otros organismos del Estado.

Las interconexiones que se materialicen por los organismos indicados en los incisos anteriores, darán derecho a los titulares de datos para que ejerzan los derechos del Título Segundo de esta ley ante cualquiera de los órganos del Estado que compartan los datos o ante el responsable de las técnicas o medios a través de los cuales se cedan los datos personales.

Artículo 35

Comunicación de sanciones

Los organismos públicos que sometan a tratamiento datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias, no podrán comunicarlos una vez prescrita la acción penal o administrativa, o cumplida o prescrita la sanción o la pena.

Exceptuase los casos en que esa información les sea solicitada por los tribunales de Justicia u otros organismos públicos dentro del ámbito de su competencia quienes deberán guardar respecto de ella la debida reserva o secreto y en todo caso les será aplicable las disposiciones de la presente ley.

Artículo 36

Bases de datos creadas y reguladas por leyes especiales

En todos aquellos asuntos en que la ley especial no regule los derechos que esta ley reconoce a los titulares o las obligaciones que se impone a los responsables y encargados, se aplicaran supletoriamente las disposiciones contenidas en esta ley.

Título VII

De la responsabilidad por las infracciones a esta ley

Artículo 37

Derecho a la indemnidad

La persona natural o jurídica privada o el organismo público responsable del tratamiento de datos personales deberá indemnizar el daño patrimonial y moral que causare por la infracción a la presente ley, 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 podrá interponerse conjuntamente con la reclamación destinada a establecer la infracción, sin perjuicio de lo establecido en el artículo 173 del Código de Procedimiento Civil. Todas las acciones se sujetarán al procedimiento sumario. El juez tomará todas las providencias que estime convenientes para hacer efectiva la protección de los derechos que esta ley establece. La prueba se apreciará en conciencia por el juez.

El monto de la indemnización será establecido por el juez de acuerdo al tipo de infracción cometida, considerando las circunstancias del caso y la gravedad de los hechos.

Artículo 38

Tipos de infracciones

Las infracciones se calificarán como leves, graves o muy graves.

Son infracciones leves:

- a) El incumplimiento del deber de información al titular cuando los datos sean recolectados del propio titular.
- b) La comunicación de los datos personales a un procesador sin dar cumplimiento a las exigencias establecidas en la ley.

Son infracciones graves:

- a) Crear bases de datos de titularidad pública o iniciar la recolección de datos personales para los mismos, sin contar con competencia legal para hacerlo.
- b) Tratar datos personales sin contar con el consentimiento de los titulares, cuando no concurra alguna de las excepciones contenidas en el artículo 4°.
- c) Tratar datos personales o utilizarlos posteriormente con infracción a los principios y derechos establecidos en el Título I y II de esta ley y las disposiciones que los desarrollan, salvo que sea constitutivo de infracción muy grave.
- d) Ceder datos personales sin contar con la legitimación para hacerlo de conformidad con esta ley, salvo que la misma sea constitutiva de infracción muy grave.
- e) La vulneración del principio de confidencialidad.
- f) El impedimento u obstaculización del ejercicio de los enumerados en el título II.
- g) No implementar las medidas de seguridad fijadas por la ley para la protección de los datos personales.
- h) La reiteración de infracciones leves.

Son infracciones muy graves:

- a) Recolectar datos personales de manera fraudulenta o engañosa.
- b) Tratar o ceder datos personales especialmente protegidos, salvo en los supuestos en que la misma ley lo autoriza.
- c) No cesar en el tratamiento ilegítimo de datos personales cuando hubiese sido determinado por los tribunales de justicia.

- d) No comunicar en la forma señalada en el artículo XX la violación de datos personales.
- e) La reiteración de infracciones graves.

Si se verifica la concurrencia de dos o más infracciones subsumibles, se aplicará la sanción correspondiente a la infracción más grave.

Artículo 39

Tipos de sanciones

Las infracciones leves serán sancionadas con multa de 100 a 1.000 UTM. Las infracciones graves serán sancionadas con multa de 1.001 a 5.000 UTM. Las infracciones muy graves serán sancionadas con multa de 5.001 a 10.000 UTM.

Las multas señaladas precedentemente se aplicarán al infractor considerando un tope equivalente al 5% de sus ventas globales en el último ejercicio comercial.

Tratándose de reiteración de infracciones muy graves, el tribunal podrá, mediante resolución fundada, aplicar como sanción accesoria la inhabilitación perpetua de la base de datos infractora.

Artículo 40

Determinación de las sanciones

Las sanciones se determinarán atendiendo a los siguientes criterios:

- a) El carácter continuado de la infracción.
- b) Los beneficios obtenidos, por el infractor o por terceros, como consecuencia de la infracción.
- c) El grado de intencionalidad.
- d) La reiteración en la comisión de infracciones.
- e) La cantidad de datos tratados por el responsable o encargado del tratamiento.
- f) La cantidad de datos personales contenidos en la base de datos infractora.
- g) La vinculación de la actividad del infractor con la realización de tratamiento de datos.
- h) Cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad en los hechos infractores.

El tribunal podrá reducir en un tope no mayor al 30% fijado de acuerdo a la gravedad de la sanción cometida, cuando el responsable o encargado demuestren que han realizado una evaluación de impacto en la protección de los datos de conformidad a las disposiciones de esta ley o han notificado a los titulares los incidentes de seguridad, ofreciendo las reparaciones adecuadas en relación a la infracción cometida. Toda otra medida de información, transparencia y rendición de cuentas, podrá ser tomada como un antecedente para determinar si existió la debida diligencia en el tratamiento de datos personales.

Artículo 41

Pago de las Multas

Las multas impuestas por el tribunal serán de beneficio fiscal y deberán ser pagadas en la Tesorería General de la República dentro de los diez días siguientes a la fecha en que la sentencia respectiva se encuentre ejecutoriada. En el mismo plazo, se debe acreditar el pago ante el tribunal.

Artículo 42 Prescripción

Las acciones para reclamar las infracciones muy graves prescribirán a los 3 años, las graves a los 2 años y las leves al año. El plazo de prescripción comenzará a contarse desde el día en que el afectado ha tomado conocimiento del hecho. En caso de infracciones continuadas, el plazo se contará desde el día en que la infracción haya cesado o se hubiere detectado por un titular.

Título Final Artículo 43

Introdúzcase la siguiente modificación a la letra d) del artículo 33 del artículo primero de la ley N° 20.285 sobre Acceso a la Información Pública:

Intercálese luego de la frase "legislación sobre transparencia y acceso a la información," la siguiente "y sobre protección de datos personales,"

Artículo 44 Deroga la ley 19.628, sobre protección a la vida privada.

¹ Claudio Ortiz, Chile, la protección de datos personales ¿Están en crisis nuestros derechos fundamentales? "Artículo: La Protección de datos personales y la información comercial". Ed. Udp. 2009 pág. 24.

² BANDA VERGARA, Alfonso. MANEJO DE DATOS PERSONALES: UN LIMITE AL DERECHO AL DERECHO A LA VIDA PRIVADA. Rev. derecho (Valdivia) dic. 2000, vol. 11, p.55-70. ISSN 0718-0950. P.55

³ Proyecto de ley de los Senadores Felipe Harboe, Pedro Araya, Eugenio Tuma, Ricardo Lagos, y Hernán Larraín.

⁴ http://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=9384-07

⁵ BANDA VERGARA, Alfonso. MANEJO DE DATOS PERSONALES: UN LIMITE AL DERECHO AL DERECHO A LA VIDA PRIVADA. Rev. derecho (Valdivia), dic. 2000, vol. 11, p.55-70. ISSN 0718-0950. P.58

⁶ <http://www.elmostrador.cl/mercados/2015/12/28/necesita-chile-una-nueva-ley-de-proteccion-de-datos/>

⁷ <http://bcn.cl/1ux0e>