INFORME DE LA COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO recaído en el proyecto de ley, en primer trámite constitucional, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales.

BOLETINES Nos. 11.092-07 y 11.144 - 07, refundidos

_____

HONORABLE SENADO:

La Comisión de Constitución, Legislación, Justicia y Reglamento tiene el honor de informar el proyecto de ley señalado en el epígrafe, iniciativa que refunde en un solo texto la Moción de los Honorables Senadores señores Harboe, Araya, De Urresti y de los ex Senadores señores Espina y Larraín, sobre protección de datos personales (Boletín N° 11.092-07), con el proyecto de ley, iniciado Mensaje de S.E. la ex Presidenta de la República, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales (Boletín N° 11.144-07).

A una o más sesiones en que se analizó este proyecto asistieron, además de los integrantes de la Comisión, el Honorable Senador señor Víctor Pérez Varela; el ex Ministro de Hacienda, señor Rodrigo Valdés; el ex Subsecretario de esta Secretaría de Estado, señor Alejandro Micco; la ex Subsecretaria de Evaluación Social del Ministerio de Desarrollo Social, señora Heidi Berner; la ex Coordinadora de Mercado de Capitales y Finanzas Internacionales del Ministerio de Hacienda, señora Bernardita Piedrabuena, quien durante el estudio de esta iniciativa pasó a desempeñarse como funcionaria del Ministerio de Economía, Fomento y Turismo; los asesores del Ministerio de Hacienda, abogados señores Roberto Godoy y Braulio Palma, y señoras Jimena Krautz y Sofía Aroca. En representación del Ministerio de Economía, Fomento y Turismo, también estuvieron presentes los asesores señores Adrián Fuentes, Andrés Pennycook y David Henríquez, y de la Subsecretaría de Evaluación Social del Ministerio de Desarrollo Social, el Jefe de la División de Políticas Sociales, señor Luis Díaz.

Concurrieron, asimismo, el ex Presidente del Consejo para la Transparencia, señor José Luis Santa María; los consejeros, señores Marcelo Drago y Jorge Jaraquemada; el Director General, señor

Raúl Ferrada; el Secretario Ejecutivo, señor José Ruiz; la Directora Jurídica, señora Andrea Ruíz; el Jefe la Unidad de Normativa, señor Pablo Contreras, y los Abogados Analistas, señores Alejandro González y Juan Baeza.

Además, expusieron ante la Comisión, el Fiscal de la Asociación de Bancos e Instituciones Financieras, señor Juan Esteban Laval; el Presidente de la Cámara Nacional de Comercio, señor Ricardo Mewes; el Gerente General De la Confederación de la Producción y del Comercio, señor Fernando Alvear; el Presidente de la Asociación Chilena de Empresas de Tecnología de información A.G., señor Raúl Ciudad; el Secretario General De la Cámara de Comercio de Santiago, señor Cristián García Huidobro; el Director Legal de EQUIFAX, señor Ignacio Bunster; la Directora Ejecutiva de la ONG Derechos Digitales, señora María Paz Canales; la Directora Ejecutiva de la Fundación de Datos Protegidos, señora Romina Garrido; el Director de Herman Consultores, señor Jorge Hermann; el Director del Centro de Estudios de Derecho Informático de la Universidad de Chile, señor Renato Jijena; el Presidente de la Fundación Pro Acceso, señor Juan Pablo Olmedo; el Director Ejecutivo de MAPCITY, señor Roberto Camhi; el Director Ejecutivo de la Asociación Latinoamericana de Internet - ALAI, señor Gonzalo Navarro; el Presidente de la Cámara Chilena Norteamericana de Comercio - AMCHAM, señor Guillermo Carey; el Gerente de Proyectos de la Asociación de Aseguradores de Chile A.G., señor Marcelo Mosso y el Gerente de Operaciones, señor Cristián Millas; el Vicepresidente del Colegio de Bibliotecarios de Chile, señor Víctor Candia; el Presidente de la Corporación Nacional de Consumidores y Usuarios (CONADECUS), señor Hernán Calderón; el abogado de Ferrada-Nehme Abogados, señor Víctor Andrade; el asesor de la Fundación Jaime Guzmán, señor Héctor Mery; el Segundo Vicepresidente del Instituto Chileno de Derecho y Tecnología, señor Alejandro Hevia; el Presidente de la Organización de Consumidores y Usuarios (ODECU), señor Stefan Larenas; el Vicepresidente Ejecutivo de Retail Financiero, señor Claudio Ortiz; el Gerente de Marketing y Productos de Transunión Chile, señor Leonardo Arancibia. el Vicepresidente de la Fundación Hacer Chile, señor Rodrigo León; la abogada de FUCATEL, señora Lorena Donoso; el Director Nacional de Protección de Datos de Argentina señor Eduardo Bertoni; el Adjunto de la Agencia Española de Protección de Datos, señor Jesús Rubí y el asesor, señor Miguel Ángel Pérez; la Directora Nacional del Instituto Nacional de Estadísticas, señora Ximena Clark; el Presidente de la Asociación de Telefonía Móvil – ATELMO, señor Guillermo Pickering; el Consejero y Presidente del Comité de Innovación de la Sociedad de Fomento Fabril, señor Raúl Ciudad; la Gerente de Políticas Públicas de Google, Cono Sur, señora Eleonora Rabinovich; el socio de Destácame, señor Augusto Ruiz-Tagle.

En representación de la Confederación de la Producción y del Comercio, asistió el abogado, señor Christian Acuña. De la Cámara Nacional de Comercio, concurrieron el abogado, señor Christian Acuña y el asesor, señor Carlos Acuña. De la Asociación Chilena de

Empresas de Tecnología de información A.G., estuvo presente el abogado señor Alex Pessó. De la Cámara de Comercio de Santiago, la abogada, señora Alejandra Velasco. De EQUIFAX, el Gerente General, señor Carlos Johnson. De la ONG Derechos Digitales, el analista de políticas públicas, señor Pablo Viollier. De Herman Consultores, el abogado, señor Alejandro Arriagada. Del Centro de Estudios de Derecho Informático de la Universidad de Chile, la abogada, señora Daniela Vásquez. De la Cámara Chilena Norteamericana de Comercio (AMCHAM), la Gerente de Contenidos, señora Tatiana Molina y la especialista de datos, señora Paulina Silva. De la Asociación de Aseguradores de Chile A.G., el abogado, señor Francisco Serqueira. Del Colegio de Bibliotecarios de Chile, la señora Claudia Cuevas. De la Corporación Nacional de Consumidores y Usuarios (CONADECUS), la abogada, señora Ximena Orrego. De Ferrada-Nehme Abogados, el abogado, señor Víctor Andrade. Del Instituto Chileno de Derecho y Tecnología, la Secretaria y Consejera, señora Alejandra Moya y los Consejeros, señora Alejandra Hevia y señor Carlos Reusser. De la Organización de Consumidores y Usuarios (ODECU), la Periodista, señora Bárbara Ipinza. Del *Retail* Financiero, el Gerente de Asuntos Corporativos, señor Javier Vega. De Transunión Chile, el Gerente de *Marketing* y Productos, señor Leonardo Arancibia. De la Fundación Hacer Chile, el Vicepresidente, señor Rodrigo León. De FUCATEL, la abogada, señora Lorena Donoso. Del Instituto Nacional de Estadísticas, la Asesora Legislativa, señora Danielle Zaror y la Asesora de Comunicaciones, señora Alejandra Peña. De la Asociación de Telefonía Móvil (ATELMO), el Gerente de Relaciones Institucionales y Estratégicas, señor Cristián Sepúlveda, el Gerente de Regulación, señor José Ignacio González y el abogado, señor José Ignacio Ceja. De la Sociedad de Fomento Fabril, la Abogada Jefe de Asuntos Regulatorios, señora Cecilia Flores.

De igual manera, asistieron los lobbistas o gestores de intereses particulares de la Cámara Nacional de Comercio y de García Magliona y Cía. Abogados, señores Nicolás Yuraszeck y Luis Ferreira. Representando a Evans Espiñeira Consultores, la Cientista Política, señora Javiera Campo. Finalmente, por la empresa Imaginaccion, la consultora de asuntos públicos, señora Beatriz Sanhueza; la cientista política, señora Carolina Salas y la consultora, señora Denise Schlesinger.

Asimismo concurrieron en representación del Ministerio Secretaría General de la Presidencia, las ex asesoras, señoras Elvira Oyanguren, María Paz Barriga, Vanessa Astete y Constanza González y los ex asesores señores Guillermo Briceño, Giovanni Semería, Vicente Manríquez, Ignacio Cárcamo, Hernán Campos y Luis Batallé. Del Ministerio de Justicia y Derechos Humanos, la ex asesora jurídica, señora Loreto Neumann. Del Ministerio Público, las abogadas, señoras Carolina Cruzat, Erika Flores, Alejandra Seguel e Ivonne Sepúlveda y el abogado, señor Francisco Aravena. Del Centro Nacional de Análisis Criminal de la Policía de Investigaciones de Chile, el Subcomisario, señor Ángelo Dini, el profesional,

señor Óscar Gutiérrez y la Inspectora de la Brigada Congreso Nacional, señora Constanza Lagos. De la Asociación de Funcionarios del Servicio Nacional del Consumidor, el Presidente, señor Paul Laulié. Las integrantes de la Delegación de la Unión Europea en Chile, señoras Leticia Celador y Elodie Jessu. De Comunidad y Justicia: La Asesora Legislativa, señora Simona Canepa. Las periodistas, de Pulso, señora Lucy Aravena, y del Diario Financiero, señora Denisse Vásquez.

Además, asistieron, el asesor de la Biblioteca del Congreso Nacional, señor Juan Pablo Cavada y el Investigador, señor Alejandro Gacitúa; del Grupo Bicameral de Transparencia, la asesora señora Rocío Noriega; la Jefa de Gabinete del Honorable Senador señor Harboe, señora Deborah Bailey y la asesora, señora Carolina González; los asesores del H. Senador señor De Urresti, señora Melissa Mallega y señores Juan Peña y Claudio Rodríguez; los asesores del Honorable Senador señor Espina, señores Andrés Aguilera, Fredy Vásquez, Nicolás Duhalde y Pablo Urquízar; los asesores del Honorable Senador señor Larraín, señor Juan Pablo Olmedo y señora Isidora Eyzaguirre; la asesora del H. Senador señor Girardi, señora Victoria Fullerton; los asesores del Honorable Senador señor Prokurica, señora Carmen Castañaza y el señor Alejandro López; el asesor del Comité DC, señor Robert Angelbeck; los asesores del Comité UDI, señora Teresita Santa Cruz y señores Héctor Mery, Benjamín Rug, Sebastián Sotelo y Cristóbal Alzamora; el asesor del Comité PS, señor Francisco Aedo; el asesor del Comité PPD, señor Sebastián Abarca; la asesora del Comité PPD, señora Catalina Wildner; el Jefe de Asesores del Comité PS, señor Héctor Valladares y los asesores del mismo Comité, señores Juan Peña, Francisco Aedo y Rafael Ferrada; el asesor del Comité UDI, señor Benjamín Rug, y el asesor de la Bancada PC, señor Guillermo Briceño.

-.-.-

OBJETIVO DEL PROYECTO

Perfeccionar las normas relativas al tratamiento de los datos personales de las personas naturales, de manera que éste se realice con el consentimiento del titular de dichos datos o en los casos que lo autorice la ley, asegurando estándares de calidad, información, transparencia y seguridad. Asimismo, crear la Agencia de Protección de Datos Personales, organismo público encargado de velar por la protección de los datos personales.

NORMAS DE QUORUM ESPECIAL

Hacemos presente que el inciso tercero del artículo 25 y el artículo 50, tienen rango de ley de quorum calificado, en virtud

de lo establecido en el inciso segundo del artículo 8° y el artículo 66 inciso tercero de la Constitución Política de la República.

Asimismo, que los artículos 33, incisos tercero y sexto, 47, 48, inciso sexto, 49, inciso primero, 57 y 58 tienen rango orgánico constitucional toda vez que inciden en atribuciones de órganos regidos por leyes orgánicas constitucionales, y a lo dispuesto en el artículo 66 inciso segundo de la Constitución Política de la República

CONSTANCIA REGLAMENTARIA

Cabe consignar que la Comisión acordó, por la unanimidad de sus integrantes, solicitar la autorización de la Sala del Senado para refundir en una sola iniciativa los siguientes proyectos de ley: (1) Moción de los Honorables Senadores señores Harboe, Araya, De Urresti, Espina y Larraín, sobre protección de datos personales (Boletín N° 11.092-07), y (2) Mensaje de S.E. la Presidenta de la República, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales (Boletín N° 11.144-07).

Al fundamentar esta petición, se tuvo presente que ambas iniciativas tienen ideas matrices comunes y se encuentran en primer trámite constitucional. Asimismo, se consultó el parecer de sus autores, dando cumplimiento a lo que dispone el artículo 17 A de la Ley Orgánica Constitucional del Congreso Nacional.

Igualmente solicitó que, en caso de autorizarse lo anterior, se le permitiera discutir en general y en particular ambos proyectos, en el trámite de primer informe de Comisión, con el fin de proponer un solo texto para la discusión en general de este proyecto por parte del Senado.

Con fecha 22 de marzo de 2017, la Sala del Senado accedió a ambas peticiones.

Hacemos presente que durante el estudio de estas iniciativas la Comisión recibió una serie de sugerencias de redacción elaboradas por un grupo de asesores parlamentarios, integrado por las señoras Melissa Mallega y Catalina Wildner, y los señores Sebastián Abarca, Robert Angelbeck, Héctor Mery, Juan Pablo Olmedo y Pablo Urquízar, quienes formularon un conjunto de proposiciones que fueron consideradas durante el estudio de este asunto.

Esta instancia trabajó conjuntamente con los asesores del Ministerio de Hacienda, señor Roberto Godoy y del Ministerio de Economía, Fomento y Turismo, señora Bernardita Piedrabuena.

Finalmente, el Ejecutivo presentó un conjunto de indicaciones que fueron consideradas y votadas por la Comisión, según se da cuenta en los acápites siguientes de este informe.

ANTECEDENTES

I.- de Derecho.

Se relacionan con esta iniciativa las siguientes normas:

1.- Norma Constitucionales.

1.1.- El artículo 8°, inciso segundo, que establece que son públicos los actos y resoluciones de los órganos del Estado, así como sus fundamentos y los procedimientos que utilicen.

1.2 - El artículo 19 N° 4 que asegura a toda persona el respeto y protección a la vida privada y a la honra de la persona y su familia.

1.3.- El artículo 19 N° 5 que asegura a toda persona la inviolabilidad del hogar y de toda forma de comunicación privada.

1.4.- El artículo 19 N° 12 que asegura a toda persona la libertad de emitir opinión y de informar, sin censura previa, en cualquier forma y por cualquier medio.

2.- Normas legales

2.1.- Ley N°19.628, sobre protección de la vida privada.

2.2.- Ley N° 20.285, sobre acceso a la información pública.

II.- de Hecho

Tal como se consignó precedentemente, el proyecto de ley que se somete a la consideración de la Sala se ha elaborado a partir de dos iniciativas de ley que se han refundido en un solo texto, según se propondrá en un acápite posterior de este informe. Las mencionadas iniciativas son las siguientes:

2.1. Moción de los Honorables Senadores señores Harboe, Araya, De Urresti, Espina y Larraín, sobre protección de datos personales. (Boletín N° 11.092-07).

En los fundamentos de esta iniciativa se afirma que la protección de los datos personales constituye un derecho autónomo.

Se precisa que la protección de datos personales es 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.

Añade 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.

Seguidamente, precisa que si bien el derecho a la protección de datos es una derivación del derecho a la intimidad debe ser reconocido como un derecho autónomo y de tercera generación.

Explica que este derecho 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. En particular, 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.

Luego, esta moción se refiere a la legislación chilena en el contexto global

En esta materia destaca que 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.

Seguidamente puntualiza que la protección de datos en Chile se ha visto severamente cuestionada, en especial por la falta de certezas sobre tratamiento del flujo de información. Por otra parte, destaca que 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 encuentran un contrapeso en una institucionalidad protectora con respuestas efectivas y disuasivas de dichas conductas. Lo anterior, explican redunda en que Chile no tiene un nivel no adecuado de protección en materia de datos personales por lo que ha debido someterse al mecanismo de cláusulas tipo en los respectivos contratos que se suscriben con empresas extranjeras.

A continuación, señala que Ley de Protección a la Vida Privada (ley N°19.628), si bien contiene una serie de principios y garantías, no está 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.

Destaca que a nivel comparado el resguardo 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, además, tienen una Autoridad de Control con distintos estándares.

Si bien Chile aprobó ley N° 19.628 el año 1999, con la que fue pionero en la región, hoy en día es insuficiente e inferior al de países vecinos. Así, por ejemplo, países como Argentina, Uruguay, Perú, Costa Rica y México han avanzado en esta materia y han logrado cumplir con los estándares europeos en esta materia.

Recuerda que en nuestro país 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, ellos no han tenido un 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, no ha alcanzado un consenso político en torno al tipo de modelo de institucionalidad y a los recursos que significarían al erario público.

En seguida indica que 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.

Añade que 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, como son: 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, explica que la magnitud de la recolección y el 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 se debe facilitar la libre circulación de los datos, es necesario garantizar un adecuado nivel de protección a los mismos.

En síntesis, plantea que el país no cuenta con una legislación adecuada, esto es una ley que exprese adecuadamente el principio rector en materia de protección de datos: el control. Indica que nuestra ley está desactualizada, dado que no fue concebida para proteger derechos de las personas.

Seguidamente explica que son varios los estándares que es posible adoptar, optándose en la presente moción, por el más alto de ellos, el Reglamento Europeo de Protección de Datos N° 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.

A partir de estos antecedentes señala que la idea matriz de esta iniciativa es establecer un nuevo marco normativo que se ajuste a los estándares exigidos por las legislaciones más modernas. En este sentido, la presente moción propone una serie de avances en cuanto los organismos que se sujetan a sus normas

A continuación, explica que el texto se estructura de la siguiente manera:

- Cambia la actual ley de protección a la vida privada poniendo en el centro de la misma 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.

- Aumenta 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. Asimismo 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 obligaciones a quienes desempeñan las funciones de responsable, corresponsable y encargado.

- Señala expresamente obligaciones como las relativas a la seguridad de los datos.

- Establece normas 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.

No obstante lo anterior, precisa que, por corresponder a una materia de la iniciativa exclusiva del Ejecutivo, no es posible abordar en este proyecto de ley cuestiones básicas como la creación de una autoridad de supervisión y control en esta materia, que entregaría a nuestro país un régimen adecuado de amparo, mejorando considerablemente la calidad de la protección de los derechos de las personas. En consecuencia, puntualiza, 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 se establece 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.

Finalmente, indica que mientras no se cuente con una institucionalidad moderna y especializada, con un diseño independiente del ciclo político 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 mantendrá un sistema de vulneración de garantías fundamentales, y de aquellos que derechos no están reconocidos en el texto de la legislación vigente.

2.2.- Mensaje de S.E. la Presidenta de la República, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. Boletín N° 11.144-07.

En los antecedentes que sirven de fundamento a esta iniciativa se explica que el mundo avanza hacia el desarrollo de la economía digital. Agrega que asistimos a cambios y transformaciones sociales, culturales y tecnológicas de extraordinaria envergadura. Estamos, en un proceso de transición desde la sociedad industrial a la sociedad digital.

Precisa que la sociedad digital ha expandido los espacios de libertad, autonomía y desarrollo de las personas, pero también ha diseñado nuevos y sofisticados sistemas de control y vigilancia que amenazan o limitan esa misma libertad.

Agrega que esta nueva realidad obliga a las sociedades y a los gobiernos a crear reglas de conducta que permitan organizar las transformaciones en la sociedad digital. Asimismo, exige la adaptación de las regulaciones, prácticas, instituciones y la organización industrial y productiva de las empresas al uso generalizado de las tecnologías de la información.

Luego, afirma que si bien la expansión de la economía digital tiene efectos positivos para el bienestar de los ciudadanos, ella enfrenta barreras o restricciones en el acceso y uso de las nuevas tecnologías de la información y en la existencia de hábitos y prácticas culturales que enfatizan el uso de sistemas análogos por sobre los sistema digitales. Esto se explica por la desconfianza que los consumidores tienen respecto de la seguridad relativa al cumplimiento de los requisitos de autenticidad, integridad y confidencialidad de las operaciones y sus registros, y a la falta de un marco normativo adecuado y de instituciones eficaces para sancionar las infracciones y resolver las controversias.

Añade que otra restricción que se puede observar en esta materia se vincula con la configuración de los mercados y las conductas de los agentes económicos. Muchas empresas mantienen

prácticas que no son compatibles con sistemas abiertos, competitivos y transparentes propios de una economía digital.

Puntualiza que Chile es una economía pequeña pero abierta al mundo. Para que mantenga esta característica e incremente su trayectoria de desarrollo y crecimiento económico, es necesario emprender cambios y transformaciones que permitan avanzar hacia una economía más innovadora, especialmente en el ámbito de los servicios globales.

Una de las mayores deudas en materia regulatoria es la falta de una legislación moderna y flexible que permita cumplir las normas y estándares internacionales en materia de protección y tratamiento de los datos personales.

Luego, hace presente que esta iniciativa recoge las recomendaciones que la OCDE ha puesto a disposición de los países miembros. Entre ellas, destacan las directrices sobre protección de la privacidad y flujos transfronterizos de datos personales.

Seguidamente, se refiere al derecho a la vida privada y su protección. En este aspecto recuerda que la Constitución Política de la República garantiza el derecho a la vida privada y su protección.

Asimismo, señala que la Declaración Universal de los Derechos Humanos de las Naciones Unidas prescribe que nadie sufrirá injerencias arbitrarias en su vida privada, su familia, domicilio o correspondencia, ni ataques a su honra o reputación.

Menciona que la Convención Americana sobre Derechos Humanos, denominada “Pacto de San José de Costa Rica”, consagra la protección de la honra y la dignidad de la persona, prohibiendo injerencias arbitrarias en su vida privada.

Explica que bajo este marco constitucional e internacional se dictó la ley N° 19.628, sobre protección de la vida privada, que establece las normas que actualmente regulan la protección y el uso de los datos de carácter personal de las personas naturales, tanto en sus aspectos sustantivos como procedimentales.

Asevera que si bien ese cuerpo legal constituyó en el pasado un gran avance, es necesario modernizarlo para hacer frente al acelerado desarrollo tecnológico, la masificación en el uso de las tecnologías de la información, el extendido acceso a internet, la expansión del comercio electrónico, unido a los nuevos desafíos que enfrentan las sociedades y los Estados para reconocer y proteger los derechos de sus ciudadanos.

Añade que para elaborar este proyecto se han tenido a la vista diversas iniciativas de ley; los estudios que realizado la Unidad de Evaluación de la Ley de la Cámara de Diputados sobre los impactos y desafíos de la ley N° 19.628, y la jurisprudencia de la Excma. Corte Suprema en esta materia.

Igualmente explica que se ha considerado el aporte del sector privado a este debate, destacando las contribuciones técnicas realizadas por el Consejo de la Sociedad Civil de Economía Digital y la Mesa Público Privada de Protección de Datos.

En este marco afirma que esta iniciativa busca balancear y equilibrar las diferentes miradas y opciones técnicas, económicas, jurídicas y políticas que han promovido los diferentes sectores, sin entrabar ni entorpecer la libre circulación de la información y, así elaborar una legislación moderna y flexible en materia de protección de datos.

Luego se refiere al objetivo de este proyecto. Al respecto indica que tiene por propósito general actualizar y modernizar el marco normativo e institucional relativo al tratamiento de los datos personales de las personas naturales, de manera que éste se realice con el consentimiento del titular de datos o en los casos que autorice la ley, asegurando estándares de calidad, información, transparencia y seguridad.

Agrega que el proyecto pretende equilibrar el respeto y protección a la vida privada e intimidad, con la libre circulación de la información.

A continuación indica los objetivos específicos que persigue esta iniciativa:

1. Establecer las condiciones regulatorias que permitan reforzar los derechos de los titulares de datos personales en relación a las operaciones de tratamiento de datos que legítimamente efectúen los agentes privados y públicos.

2. Dotar al país de una legislación moderna y flexible en materia de tratamiento de datos personales, que sea consistente con los compromisos internacionales adquiridos luego de su incorporación a la OCDE y ajustada a las normas y estándares internacionales.

3. Incrementar los estándares legales de Chile en el tratamiento de datos personales para transformarlo en un país con niveles adecuados de protección y seguridad, promoviendo el desarrollo de la economía digital y favoreciendo la expansión del mercado de los servicios globales.

4. Definir modelos regulatorios, condiciones operacionales y un marco institucional que legitime el tratamiento de los datos personales por parte de los órganos públicos, garantizando el cumplimiento de la función pública y los derechos de los ciudadanos.

5. Contar con una autoridad de control de carácter técnico y una institucionalidad pública que asuma los desafíos regulatorios y de fiscalización en materia de protección de las personas y tratamiento de los datos personales.

En seguida, el mensaje se refiere al contenido del proyecto.

Indica que el objeto del mismo es regular el tratamiento de los datos personales, asegurando el respeto y protección de los derechos y libertades fundamentales de los titulares de datos (personas naturales), en particular el derecho a la vida privada.

Explica que su ámbito de aplicación es todo tratamiento de datos personales que realicen las personas naturales o jurídicas, incluidos los órganos públicos, que no se encuentre regido por una ley especial. En todo caso, precisa que esta normativa tendrá el carácter supletorio de todos aquellos tratamientos de datos regulados en leyes especiales.

Añade que se excluyen de este régimen regulatorio al tratamiento de datos personales que se realice en el ejercicio de las libertades de emitir opinión y de informar regulado por las leyes especiales dictadas de conformidad al numeral 12 del artículo 19 de la Constitución Política de la República, y el tratamiento que efectúen las personas naturales en relación con sus actividades personales.

Asimismo, indica que esta iniciativa no innova respecto de la regulación específica y actualmente vigente, referida al tratamiento de los datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial, manteniendo íntegramente las normas contenidas en el Título III de la ley 19.628, salvo adecuaciones formales y de referencia.

Seguidamente puntualiza que este proyecto incorpora un conjunto de principios rectores en materia de protección y tratamiento de los datos personales que han sido reconocidos en las directrices de la OCDE y en la legislación comparada. Estos principios son la licitud del tratamiento, finalidad, proporcionalidad, calidad, seguridad, responsabilidad e información.

En el tratamiento de datos personales por parte de los organismos públicos se incorporan además los principios de coordinación, eficiencia, transparencia y publicidad.

Agrega que para facilitar a los operadores del sistema la aplicación e interpretación de la ley, se actualizan e incorporan nuevas definiciones legales, adaptándolas a las que se usan en las legislaciones más modernas, y las recomendaciones técnicas de los organismos internacionales

A continuación, explica que esta iniciativa busca reforzar y ampliar los derechos de los titulares de datos.

Se reconocen al titular de datos personales los derechos de acceso, rectificación, cancelación y oposición, los denominados “derechos ARCO”. Estos derechos son irrenunciables, gratuitos y no puede limitarse su ejercicio en forma convencional.

El derecho de acceso permite solicitar y obtener confirmación acerca de si sus datos personales están siendo tratados por el responsable y acceder a ellos, en su caso. El derecho de rectificación busca que se modifique o completen los datos cuando sean inexactos o incompletos. El derecho de cancelación persigue que se supriman o eliminen los datos del titular por las causales previstas en la ley. El derecho de oposición permite requerir que no se lleve a cabo un tratamiento de datos determinado por la concurrencia de las causales previstas en la ley.

Para proteger estos derechos se establece un procedimiento directo y eficaz para que cualquier titular de datos pueda recurrir directamente ante el responsable de datos permitiéndose bloquear transitoriamente los datos en cuestión. Si el responsable no acoge la solicitud o no responde dentro del plazo que le fija la ley, el titular puede presentar un reclamo ante la autoridad de control. La resolución de la autoridad de control es reclamable ante la Corte de Apelaciones respectiva.

Luego, explica que siguiendo las tendencias regulatorias más modernas se introduce el derecho a la portabilidad de los datos personales, en virtud del cual el titular de datos puede solicitar y obtener del responsable en un formato electrónico estructurado, genérico y de uso habitual, una copia de sus datos personales y comunicarlos o transferirlos a otro responsable de datos.

Por otro lado, esta iniciativa también incorpora y refuerza la regulación del denominado “derecho al olvido” en relación a los datos relativos a infracciones penales, civiles, administrativas y disciplinarias.

En seguida, precisa que el consentimiento es la fuente principal de legitimidad del tratamiento de los datos personales.

Este consentimiento debe ser libre, informado, inequívoco, y otorgado en forma previa al tratamiento y específico en cuanto a su finalidad o finalidades.

Esta regla considera excepciones tales como cuando la información ha sido recolectada de una fuente de acceso público; cuando sean datos relativos a obligaciones de carácter económico, financiero, bancario o comercial; o cuando el tratamiento sea necesario para la ejecución o el cumplimiento de una obligación legal o de un contrato en que es parte el titular.

En seguida se refiere al régimen de deberes de los responsables de datos.

Al respecto se crean una serie de obligaciones y deberes para los responsables de datos, tales como acreditar la licitud del tratamiento que realizan; deberes de información; deberes de reserva y confidencialidad, de información y transparencia, y el deber de adoptar medidas de seguridad y reportar las vulneraciones dichas medidas.

Por otro lado, para no entrabar la circulación de información, se establecen estándares diferenciados de cumplimiento de los deberes de información y de seguridad para personas naturales y jurídicas, el tamaño de la empresa y el volumen y las finalidades de los datos que trata.

También se refiere a la cesión o transferencia de las bases de datos personales.

Agrega que una de las principales innovaciones de esta nueva normativa es la regulación del tratamiento automatizado de grandes volúmenes de datos, o "*Big Data*", protegiendo la facultad de control del titular sobre su propia información, pero reconociendo también la licitud del acceso y uso de la información por parte de terceros y particularmente, de las empresas.

A continuación, el mensaje explica los nuevos estándares para el tratamiento de datos sensibles y categorías especiales de datos personales.

Al respecto precisa que se eleva el estándar para el tratamiento de los datos sensibles, estableciendo que sólo puede realizarse cuando el titular de un dato consienta libre e informadamente en entregar este antecedente.

Se reconocen excepciones que legitiman el tratamiento de los datos personales sensibles, como cuando el titular ha hecho manifiestamente públicos su dato sensible o cuando exista, por ejemplo, una situación de emergencia médica o de salud.

Asimismo, se introducen normas especiales para el tratamiento de los datos personales relativos a la salud, los datos biométricos y los datos relativos al perfil biológico humano; para el tratamiento de datos personales con fines históricos, estadísticos, científicos y para estudios o investigaciones que atiendan fines de interés público; y para el tratamiento de los datos personales de geolocalización o de movilidad del titular.

Asimismo, el mensaje se refiere al tratamiento de datos personales de niños, niñas y adolescentes. En esta materia se establece que el tratamiento de estos datos personales solo se puede realizar atendiendo al interés superior de los niños, niñas y adolescentes y al respeto de su autonomía progresiva.

Se regula en forma diferenciada las autorizaciones de tratamiento de datos de cada uno de estos menores de edad. En el caso de los niños y niñas se requiere el consentimiento previo, específico y expreso de quien tiene a su cargo el cuidado personal. Respecto de los adolescentes, se establece que sus datos personales sensibles sólo pueden ser tratados con el consentimiento de quien tiene a su cargo el cuidado personal del adolescente. Para los demás datos personales, rigen las normas generales de autorización.

Se establece una obligación especial para los establecimientos educacionales y para las personas o entidades públicas o privadas que traten o administren este tipo de datos, incluyendo a quienes ejercen su cuidado personal, de velar por el uso lícito y la protección de la información personal que concierne a los niños, niñas y adolescentes.

Seguidamente el proyecto regula el flujo transfronterizo de datos personales

En este ámbito se incorpora una regulación específica para la transferencia internacional de datos personales, ajustándola a los estándares y recomendaciones de la OCDE.

Se distingue entre países que disponen de un marco normativo que proporciona niveles adecuados de protección de datos y aquellos que no lo poseen, entendiendo que un país posee niveles adecuados de protección de datos cuando cumple con estándares similares o superiores a los fijados en la ley chilena en materia de protección y

tratamiento de datos personales. La autoridad de control, siguiendo parámetros técnicos y los estándares de la OCDE, determinará los países que poseen una legislación adecuada.

En el caso de los países adecuados se reconoce amplia autonomía a los intervinientes para transferir datos, sujeto al cumplimiento de las reglas generales. En el caso de países no adecuados, se permite la transferencia de datos sólo en un conjunto de circunstancias que autorizan el envío de la información, bajo la responsabilidad legal de quien efectúa la transferencia de datos y con aviso previo a la autoridad de control.

El proyecto también moderniza los estándares para el tratamiento de datos personales por parte de los organismos público. Explica que este tratamiento será lícito cuando se realiza para el cumplimiento de sus funciones legales, dentro del ámbito de sus competencias y de conformidad a las normas legales correspondientes. Cumpliéndose esas condiciones, no se requiere el consentimiento del titular.

Se regula la facultad de los órganos públicos para comunicar o ceder datos personales a otros órganos públicos, siempre que la comunicación o cesión de los datos sea necesaria para el cumplimiento de funciones legales y ambos órganos actúen dentro del ámbito de sus competencias. También se reglamenta la comunicación y cesión de datos a personas o entidades privadas.

Del mismo modo, se consagran los principios que rigen el tratamiento de los datos personales por parte de los órganos públicos, los derechos que se reconocen a los titulares, la forma de ejercer estos derechos y se define un procedimiento de reclamación administrativa y de tutela judicial efectiva para el ejercicio y protección de estos derechos.

Luego se define un régimen especial de responsabilidades y sanciones para proteger estos principios y reglas.

Se establece un régimen de excepción para el tratamiento de datos protegidos por normas de secreto o confidencialidad; cuando se refiere al tratamiento de datos vinculados a la investigación de infracciones penales, civiles y administrativas; cuando correspondan a actividades relacionadas con la seguridad de la nación, el orden público o la seguridad pública, y cuando en los casos que se hayan declarado estado de catástrofe o estado de emergencia.

Por último, se norma las actividades de tratamiento de los datos personales que efectúan el Congreso Nacional, el Poder Judicial, la Contraloría General de la República, el Ministerio Público, el Tribunal Constitucional, el Banco Central, el Servicio Electoral y la Justicia

Electoral, y los demás tribunales especiales creados por ley. Se contempla un modelo regulatorio, de fiscalización y cumplimiento compatible con la autonomía de estas instituciones.

En otro orden de materias, el proyecto crea una autoridad de control encargada de velar por la protección de los derechos y libertades de las personas titulares de datos.

Esta unidad estará dotada de facultades para regular, supervisar, fiscalizar y en última instancia, sancionar los incumplimientos de la ley.

Para alcanzar este objetivo se crea una institución especializada y de carácter técnico, denominada “Agencia de Protección de Datos Personales”, cuyo objetivo es velar y fiscalizar el cumplimiento de esta normativa. Ella se relaciona con el Presidente de la República a través del Ministerio de Hacienda y se encuentra afecto al Sistema de Alta Dirección Pública.

Con el objeto de evitar o precaver conflictos de normas y asegurar la coordinación, cooperación y colaboración entre la Agencia de Protección de Datos Personales y el Consejo para la Transparencia, se consagra un modelo de coordinación regulatoria entre ambas instituciones.

Seguidamente, el proyecto se refiere al modelo general de cumplimiento de la ley. En este ámbito se considera un catálogo específico de infracciones a los principios y obligaciones establecidos en la ley. Ellas que se califican en leves, graves y gravísimas, estableciendo sanciones correlativas a la gravedad de la infracción que van desde la amonestación escrita a multas que oscilan entre 1 y 5.000 UTM. En casos excepcionales se contempla el cierre o clausura de las operaciones de tratamiento de datos.

La determinación de las infracciones y la aplicación de la sanción respectiva corresponden a la Agencia de Protección de Datos Personales. En el caso de los órganos públicos y de los agentes de la Administración del Estado, las investigaciones las realiza la Agencia y las sanciones las aplica la Contraloría General de la República.

Se incorpora, asimismo, un procedimiento de reclamación judicial de ilegalidad para cualquier persona natural o jurídica que se vea afectada por una resolución de la Agencia de Protección de Datos Personales, ante la Corte de Apelaciones correspondiente. Para el conocimiento y resolución de estas controversias se establece un procedimiento judicial concentrado y de rápida resolución.

Finalmente, como una forma de incentivar y promover el cumplimiento de la ley, y siguiendo las recomendaciones de la OCDE, se regula la adopción por parte del sector privado y del sector público de modelos de prevención de infracciones, fijando para ellos los estándares y requisitos mínimos con los que deberán cumplir.

La certificación y supervisión de estos programas estará a cargo de la Agencia de Protección de Datos Personales.

El proyecto concluye con un conjunto de disposiciones transitorias. En ellas se establece que la ley entrará en vigencia el día primero del mes décimo tercero posterior a su publicación en el Diario Oficial.

Los reglamentos que contempla esta iniciativa deberán dictarse dentro de los seis meses posteriores la publicación.

Se establece un plazo de nueve meses para que, mediante uno o más decretos con fuerza de ley, el Presidente de la República regule al personal de la Agencia de Protección de Datos Personales.

Finalmente, se prescribe que dentro de los 60 días siguientes a la publicación de la ley deberá convocarse al concurso público para nombrar al primer director o directora de la Agencia de Protección de Datos Personales.

Informe de productividad

Por último, hacemos presente que esta iniciativa cuenta con un informe de productividad, elaborado por el Ministerio de Hacienda, que da cuenta del problema que se quiere abordar con esta normativa, los objetivos de la misma, las alternativas de política pública que se tuvieron presente al momento de elaborar este proyecto, los beneficios que se obtendrán con la aprobación de este cuerpo legal y los posibles costos de la misma.

Dicho informe se acompaña como anexo al presente informe.

2.3.- INFORMES DE LA CORTE SUPREMA

- Boletín N° 11.092-07

El día 14 de marzo de 2017, se dio cuenta en el Senado del oficio N° 34, de 13 de marzo de 2017, de la Excma. Corte Suprema en que comunica su parecer sobre esta iniciativa.

En dicho informe se señala, en lo esencial, lo siguiente:

“Segundo: Que el desarrollo de la red mundial de Internet y la evolución de las tecnologías de la información, que tiene implicancias de orden social, económico y cultural, sirve de contexto al proyecto de ley de que se trata, el cual propone modificar la regulación del sistema de protección de datos personales actualmente resguardado con la vigencia de la ley N° 19.628, de manera que permita ajustar este marco normativo a los estándares exigidos por las legislaciones más modernas.

En esta línea, los autores indican que la presente moción propone los siguientes avances:

i. Cambia el foco de la actual ley de protección a la vida privada poniendo en el centro a las personas.

ii. 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.

iii. Mejora el catálogo de definiciones

iv. Acota las excepciones al consentimiento respecto del tratamiento con finalidades diversas.

v. Especifica el catálogo de principios.

vi. Mejora el catálogo de derechos.

vii. 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.

viii. Incorpora responsabilidades a los roles de responsable, corresponsable y encargado.

ix. Señala expresamente las obligaciones tan importantes como las relativas a la seguridad de los datos.

x. Establece normas claras sobre tratamiento de datos comerciales.

xi. Aclara algunos aspectos relacionados con el tratamiento de datos realizados por organismos públicos.

xii. Incorpora un catálogo de infracciones y sanciones.

Tercero: Que si bien la propuesta deroga completamente la ley N° 19.628, a través de su artículo 44, verdaderamente corresponde a una actualización y refundición de los títulos y párrafos de esa ley. De este modo, con el proyecto coexisten:

i. Disposiciones que reiteran las normas de la ley N° 19.628 (v.gr. el artículo 35 del proyecto es prácticamente idéntico al artículo 21 de la normativa vigente),

ii. Disposiciones que alteran o adicionan los efectos de las normas actualmente vigentes (v.gr. el apartado de definiciones que contiene el artículo 3 del proyecto con respecto a lo dispuesto en el artículo 2 de la ley del ramo),

iii. Disposiciones inéditas, completamente inexistentes en la normativa actual (v.gr. lo dispuesto en el artículo 2 del proyecto sobre el ámbito de aplicación territorial de la ley) y,

iv. Ámbitos normativos que antes poseían una reglamentación específica, pero que en el proyecto son omitidos (v.gr. como resulta de la inexistencia en el proyecto de un artículo equivalente al artículo 3 de la ley N° 19.928).

Cuarto: Que otro asunto de carácter general, consiste en que el proyecto no crea bases institucionales y orgánicas que rijan el sistema de protección de datos personales. Esta carencia del proyecto es explicada en la moción en las limitaciones de las facultades de los senadores en materia de iniciativa legal, que les habría impedido corregir el que parece ser uno de los defectos más importantes del sistema, a saber, la inexistencia de una institucionalidad adecuada en estas materias.

Respecto de este punto, cabe observar que habitualmente las normativas que regulan el derecho a la protección de los datos personales van acompañadas del establecimiento de autoridades encargadas del control o supervisión de su cumplimiento. En general, a esta institucionalidad se le entregan facultades que implican, a lo menos, contar con total independencia de los poderes políticos en el ejercicio de sus funciones y estar dotadas de atribuciones que permitan la supervisión adecuada de las normas específicas de protección de datos. En general los países que cuentan con autoridades de control con las prerrogativas señaladas cumplen con un "nivel adecuado de protección".

En tal sentido, corresponde advertir que tanto el diseño institucional previsto por la ley vigente como por el proyecto actualmente en análisis, a pesar de propiciar la introducción de nuevos principios, derechos y prerrogativas, no cumplirían con los estándares de "nivel adecuado de protección" que en materia de datos exige la comunidad internacional[1].

Quinto: Que de acuerdo al oficio remisor del señor Presidente del H. Senado, la solicitud de informe se refiere a los artículos 20, 21 y 37 del Proyecto de que se trata, los que se analizarán en los números que vienen.

Previamente, cabe consignar que el proyecto consta de cuarenta y cuatro artículos, distribuidos en siete Títulos y uno Final.

Los artículos 20 (Procedimiento General) y 21 (Interés Colectivo) constituyen el Título III, denominado “Procedimiento de reclamación”; y el artículo 37 (Derecho a la indemnidad) es parte del Título VII, denominado “De la responsabilidad por las Infracciones a esta ley”.

Sexto: Que el texto del artículo 20 es el siguiente:

“Articulo 20
Procedimiento general

[1] Debe tenerse en especial consideración la incorporación de Chile a la OCDE. El 7 de Mayo del 2010, Chile firmó el Convenio de Adhesión a la Organización para la Cooperación y el Desarrollo Económico (OCDE) y compromete plena dedicación a la consecución de los objetivos fundamentales de dicha organización. En relación con el derecho de la protección de los datos personales, la OCDE ha emitido una serie de recomendaciones, entre las que destaca la Recomendación sobre Protección de la Privacidad y Flujo Transfronterizo de Datos Personales. Las directrices, en cuanto a la implementación de medidas internas, establecen que los países miembros deben adoptar una legislación nacional adecuada, impulsar y apoyar la autorregulación ya sea mediante códigos de conducta o de otro modo; brindar los medios razonables para que los individuos ejerzan sus derechos; sancionar adecuadamente y ofrecer soluciones en caso de fallos, con el fin de cumplir las medidas de implantación y asegurar que no haya discriminación desleal hacia el sujeto de los datos

Si el responsable del registro o banco de datos no se pronunciare 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."

El artículo 20 transcrito es prácticamente igual al 16 de la Ley 19.628, vigente sobre la materia. Existen pequeñas diferencias, como por ejemplo:

- ≡ se recurre ante el juez del domicilio del titular de los datos, mientras que actualmente lo es ante el juez del domicilio del responsable;
- ≡ el titular puede solicitar de inmediato reserva de los hechos y pruebas;
- ≡ se moderniza la forma de las notificaciones y
- ≡ las sanciones se hacen más severas.
- ≡

Séptimo: Que el texto del artículo 21 es el siguiente:

"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."

El artículo 21 es nuevo y trata de proteger el interés colectivo o difuso de los titulares de datos afectados por el incumplimiento de las obligaciones establecidas en el proyecto. Sigue la línea de la Ley de Protección a los Consumidores y establece el mismo procedimiento que ella contempla para este tipo de interés, con algunas modificaciones procedimentales encaminadas a darle mayor agilidad.

Octavo: Que el texto del artículo 37 es el siguiente:

"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."

Este artículo 37 es prácticamente idéntico al artículo 23 de la Ley actual, No.19.628.

Se encuentra, como ya se dijo, dentro del Título VII, "De las responsabilidades por las infracciones a esta ley", título que contiene además una -nueva- tipificación y graduación de las infracciones (artículo 38), una tipificación de sanciones (artículo 39), criterios para

determinar las sanciones (artículo 40), normas sobre pago y destino de las multas (artículo 41) y sobre prescripción de las acciones para reclamar de las infracciones (artículo 42). Todos los artículos no consultados, pero que complementan, al parecer adecuadamente el mecanismo sancionatorio.

Noveno: Que los artículos consultados no representan alteraciones en lo orgánico ni en lo funcional de los tribunales.

La carga de trabajo que hasta ahora generan estas materias sobre los tribunales, según datos incorporados en el documento remitido por la Dirección de Estudios, es de monto menor, en especial por lo muy específico de ellas; por lo que no es dable suponer que las modificaciones que trae el proyecto vayan a aumentarla.

En síntesis puede decirse que la iniciativa objeto de este informe pretende ser un avance en materia de protección de los derechos de las personas, incorporando una serie de principios en materia de tratamiento de datos, un nuevo catálogo de derechos para los titulares de estos y ampliando la aplicación territorial de esta protección. Además, pretende mejorar los mecanismos jurisdiccionales de protección incorporando nuevos procedimientos y acciones. Todo ello representa un avance en materia de tratamiento y protección de datos personales.

Décimo: Que el tema de que se trata es complejo y necesita ser abordado desde distintos puntos de vista; por lo que no es extraño que queden aspectos sin tratar o tratados en forma incompleta. Desde esta perspectiva se hace palpable la necesidad de reformar la ley de protección actualmente vigente desde una perspectiva holística, que se desarrolle sobre la base de la institucionalidad necesaria que garantice una efectiva protección de las personas y una adecuada trasparencia en la administración del Estado. La omisión de una nueva institucionalidad, en la iniciativa analizada, es un relevante aspecto que merece ser observado y que puede generar efectos negativos en la adecuada implementación de este proyecto de ley y en la protección de los derechos de las personas.

Por estas consideraciones y de conformidad, además, con lo dispuesto en los artículos 77 de la Constitución Política de la República y 18 de la Ley N° 18.918, Orgánica Constitucional del Congreso Nacional, se acuerda informar en los términos precedentemente expresados el proyecto de ley sobre protección de datos personales.

- Boletín N° 11.144-07

El día 9 de mayo de 2017, se dio cuenta en el Senado del oficio N° 63, de 3 de mayo de 2017, de la Excma. Corte Suprema en que comunica su parecer sobre esta iniciativa.

En dicho informe se señala, en lo esencial, lo siguiente:

“Segundo: Que este proyecto de ley constituye un esfuerzo por aunar y concretar la necesidad de actualizar el modelo y la institucionalidad de la protección de datos personales en nuestro país.

Sus propósitos son análogos a los de un proyecto –originado en moción de varios señores senadores- recientemente informado por el Pleno de la Corte Suprema mediante Oficio N° 34-2017, en la medida que pretende la modificación exhaustiva de la Ley N° 19.628, actualizándola según los estándares y principios vigentes en la materia, los requerimientos de la OCDE y los de la comunidad internacional.

Tercero: Que en la motivación de la iniciativa consigna como objetivos específicos, los siguientes:

“a. Establecer las condiciones regulatorias que permitan reforzar los derechos de los titulares de datos personales en relación a las operaciones de tratamiento de datos que legítimamente efectúen los agentes privados y públicos.

b. Dotar al país de una legislación moderna y flexible en materia de tratamiento de datos personales, que sea consistente con los compromisos internacionales adquiridos luego de su incorporación a la OCDE y ajustada a las normas y estándares internacionales.

c. Incrementar los estándares legales de Chile en el tratamiento de datos personales para transformarlo en un país con niveles adecuados de protección y seguridad, promoviendo el desarrollo de la economía digital y favoreciendo la expansión del mercado de los servicios globales.

d. Definir estándares regulatorios, condiciones operacionales y un marco institucional que legitime el tratamiento de los datos personales por parte de los órganos públicos, garantizando el cumplimiento de la función pública y los derechos de los ciudadanos.

e. Contar con una autoridad de control de carácter técnico y una institucionalidad pública que asuma los desafíos regulatorios y de fiscalización en materia de protección de las personas y tratamiento de los datos personales”;

Cuarto: Que dada la notoria coincidencia de objetivos entre este proyecto y el recientemente informado por el Pleno de la Corte Suprema, cabe puntualizar que a diferencia de aquel, éste sí introduce

reformas de relevancia a nivel orgánico e institucional, creando una nueva “Agencia de Protección de Datos Personales”, subsanando, de esta manera, el mayor reparo identificado por el Pleno en el proyecto anterior.

Habida consideración de los objetivos señalados –coincidentes, como se ha dicho, con los del proyecto informado recientemente- y la evidente necesidad legislativa que existe en estas materias, el presente informe contiene principalmente observaciones respecto de las cuatro disposiciones legales cuyo comentario se solicitó por el oficio del H. Senado.

Además se entregan algunos comentarios específicos respecto de otras disposiciones, innovaciones y carencias del proyecto, que podrían impactar de modo relevante en la organización y atribuciones de los tribunales;

Quinto: Que lo consultado son específicamente los artículos 23, 25 inciso 2°, 47 y 51 que la iniciativa, propone para el texto nuevo, los que serán tratados individualmente a continuación.

Para mejor entendimiento del proyecto en informe, vale señalar que la técnica legislativa usada es la modificación de artículos, párrafos o títulos de la ley vigente, o la incorporación de normativa nueva que se intercala en ella.

Así, los artículos 23 y 25 se ubican en el Título IV (“Del tratamiento de datos personales por los órganos públicos”) que se remplaza por el N°8 del artículo Primero del proyecto ; el artículo 47, en el Párrafo Tercero (“Del Procedimiento de reclamación judicial”) y el artículo 51, en el Párrafo Quinto (“De la responsabilidad civil”), ambos párrafos del Título VII (“De las infracciones y sus sanciones, de los procedimientos y de las responsabilidades de los responsables de datos”), Título nuevo que se incorpora por el N°10 del artículo primero del proyecto a la ley N°19.628, sobre protección de la vida privada;

Sexto: Que el texto del artículo 23 propuesto por el proyecto de ley, ubicado, como se dijo, en su título IV (que regula el tratamiento de datos personales realizado por organismos públicos), es el siguiente:

“Artículo 23.- Ejercicio de los derechos del titular y reclamo de ilegalidad. El titular de datos puede ejercer ante el órgano público los derechos de acceso y rectificación que les reconoce esta ley. El titular no podrá cancelar ni oponerse al tratamiento de datos efectuado por un órgano público salvo que el tratamiento realizado sea contrario a las disposiciones de este título.

El ejercicio de los derechos del titular se deberá realizar de acuerdo al procedimiento establecido en el artículo 11 de esta ley, dirigiéndose al jefe superior del servicio. En todo lo no regulado se aplicarán supletoriamente las normas de la ley N° 19.880, que establece bases de los procedimientos administrativos que rigen los actos de la Administración del Estado.

Las personas que se vean afectadas por la resolución de un órgano público, sea que les deniegue el ejercicio de un derecho reconocido en esta ley o adopte una decisión o dicte una acto que infrinja los principios y obligaciones establecidos en ella, causándole perjuicio, podrá deducir un reclamo de ilegalidad ante la Corte de Apelaciones de Santiago o del domicilio de reclamante, a su elección, de conformidad con las normas dispuestas en el artículo 47 de esta ley. El informe a que alude la letra d) del artículo 47 será evacuado por el órgano público reclamado.

Sin perjuicio de lo anterior, la Corte de Apelaciones respectiva podrá requerir informe a la Agencia de Protección de Datos Personales con el objeto de establecer si en las operaciones de tratamiento de datos realizadas por el órgano público hubo o no infracción a los principios y obligaciones establecidos en esta ley.”.

La primera regla de la disposición, estipula que el titular de los datos personales ubicados en bases pertenecientes a órganos públicos, sólo goza del derecho a acceder y solicitar la rectificación de sus datos. Así, los derechos de oposición y cancelación se encuentran restringidos en este caso, pues el titular sólo podrá ejercerlos en la medida que identifique una infracción a alguna de las normas que componen el título IV de la propuesta. Lo que puede explicarse por la evidente asimetría de fines que suele existir entre el tratamiento de datos de una institución pública y el de una privada. Sin perjuicio de tal justificación, la norma resulta criticable en a lo menos tres sentidos distintos.

En primer lugar, en una crítica aplicable a todo el sistema del referido título IV de la propuesta, porque no se perfecciona la definición de “organismo público” actualmente contemplada por la ley N° 19.628, cuyo artículo 2° letra k) dispone que para sus efectos se entenderá por organismos públicos a “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 1º de la ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado”. Esta definición no se corresponde con el complejo diseño institucional e imbricación existente entre los organismos persecutores de fines públicos y aquellos que buscan fines privados. Así, el problema de la definición dice relación con la ambigüedad que se produce en varios ámbitos,

en los que el estatus de público o privado de los organismos no resulta tan claro, lo que complica la aplicación de la normativa, por ejemplo:

i. El estatus de organismo privado de aquellos prestadores de servicios privados que cumplen fines públicos críticos, ya sea porque los prestan directamente a la población (como podría ser una específica empresa concesionaria) o porque los prestan de manera directa a servicios públicos que tercerizan determinadas labores que les son propias (como sucede con la empresa que confeccionar los documentos de identificación para el Registro Civil);

ii. El estatus de organismo privado atribuible a algunas empresas estatales creadas por ley (Televisión Nacional de Chile); y

iii. El estatus de otras reparticiones públicas que, sin estar contenidas en la Constitución ni en las hipótesis del artículo 1° de la Ley N° 18.575, sí pueden entenderse incorporadas en la categoría de organismos públicos, como la Comisión de Beneficio de Reducción de Condena (comisión de composición mixta, con participación del ejecutivo y el poder judicial, creada por la ley N° 19.856 y que realiza tratamientos de bases de datos para arribar a sus conclusiones), o el Panel de Expertos en materia eléctrica.

En segundo lugar, el artículo en cuestión resulta observable en la medida que no especifica claramente si el titular de un dato contenido en una base de datos perteneciente a un organismo público puede ejercer libremente su derecho a la portabilidad.

La portabilidad de datos es un derecho actualmente inexistente a nivel legislativo, que el proyecto introduce y reconoce en su artículo 9° en los siguientes términos:

“Derecho a la portabilidad de los datos personales. El titular de datos tiene derecho a solicitar y recibir del responsable una copia de los datos personales que le conciernen de manera estructurada, en un formato genérico y de uso común que permita ser operado por distintos sistemas, y a comunicarlos o transferirlos a otro responsable de datos”.

Así, la omisión de esa modalidad de tratamiento, deja abierta la pregunta de si un titular de datos puede solicitar de un organismo público la entrega “en un formato electrónico estructurado, genérico y de uso habitual, una copia” de sus datos personales, o dicha posibilidad se encuentra vedada o limitada de alguna manera.

En tercer lugar, y aun asumiendo las características propias del sector público, la limitación de las facultades de oposición y cancelación podría resultar inestimable, si se considera que si

bien muchas bases de datos empleadas por organismos públicos sirven a fines públicos específicos, no es menos cierto que otras pueden ser construidas o empleadas con algún fin diverso. De este modo, aunque tiene sentido restringir el derecho de oposición y cancelación respecto de bases de datos construidas o tratadas en ejercicio de fines públicos, el límite que se dibuja entre los fines puramente públicos y los intereses privados está difuso en la estructura del proyecto, haciendo que la restricción parezca excesiva respecto de aquellas bases y modos de tratamiento que exceden este ámbito.

El inciso segundo del citado artículo, profundiza en la regulación de los derechos de rectificación y acceso, señalando que su ejercicio deberá someterse a lo dispuesto en el artículo 11 de la ley, aplicándose supletoriamente las normas de la ley N° 19.880. Si bien esta disposición no aparece como problemática, cabe alertar sobre la vinculación entre esta última ley y los mecanismos de la ley N° 20.285 (sobre acceso a la información pública), para efectos de disminuir las diferentes vías de reclamo disponibles para la ciudadanía, evitando la burocratización y el desvanecimiento de los canales de información, para entregar un servicio más expedito y de mejor calidad a los ciudadanos.

Los incisos 3° y 4° de este artículo, establecen un verdadero recurso contencioso administrativo en relación a la protección de los datos personales, materia en la que debe recordarse que ya existe opinión de la Corte Suprema; pudiendo señalarse al efecto el acápite cuarto del Acta N° 176-2014, que expresa: “se propone realizar una modificación legal en orden a igualar los procedimientos especiales contenciosos administrativos que hoy se aplican. En este sentido, se solicita al Ejecutivo considerar el catálogo de leyes que se puntualizan en documento anexo y que dan cuenta de las disposiciones de esa naturaleza que en nuestro ordenamiento jurídico regulan el contencioso especial en forma dispersa e inarmónica, a fin de estudiar la modificación de la competencia del tribunal que conocerá de dichas causas y respecto del procedimiento aplicable a ellas. Así, se propone entregar la competencia de los procesos contenciosos administrativos especiales, en primera instancia, a las Cortes de Apelaciones que correspondan según las reglas generales, debiendo tramitarse las respectivas causas de acuerdo al procedimiento de ilegalidad municipal contemplado por el artículo 151 letras d) a i) del D.F.L. N° 1/2006, del Ministerio del Interior, que fija el texto refundido, coordinado y sistematizado de la Ley N° 18.695, Orgánica Constitucional de Municipalidades”;

Séptimo: Que el procedimiento fijado por los referidos literales del artículo 151, dispone que:

“d) Rechazado el reclamo en la forma señalada en la letra anterior o por resolución fundada del alcalde, el afectado podrá

reclamar, dentro del plazo de quince días, ante la corte de apelaciones respectiva.

El plazo señalado en el inciso anterior se contará, según corresponda, desde el vencimiento del término indicado en la letra c) precedente, hecho que deberá certificar el secretario municipal, o desde la notificación que éste hará de la resolución del alcalde que rechace el reclamo, personalmente o por cédula dejada en el domicilio del reclamante.

El reclamante señalará en su escrito, con precisión, el acto u omisión objeto del reclamo, la norma legal que se supone infringida, la forma como se ha producido la infracción y, finalmente, cuando procediere, las razones por las cuales el acto u omisión le perjudican;

e) La corte podrá decretar orden de no innovar cuando la ejecución del acto impugnado le produzca un daño irreparable al recurrente;

f) La corte dará traslado al alcalde por el término de diez días. Evacuado el traslado o teniéndosele por evacuado en rebeldía, la corte podrá abrir un término de prueba, si así lo estima necesario, el que se regirá por las reglas de los incidentes que contempla el Código de Procedimiento Civil;

g) Vencido el término de prueba, se remitirán los autos al fiscal judicial para su informe y a continuación se ordenará traer los autos en relación. La vista de esta causa gozará de preferencia;

h) La corte, en su sentencia, si da lugar al reclamo, decidirá u ordenará, según sea procedente, la anulación total o parcial del acto impugnado; la dictación de la resolución que corresponda para subsanar la omisión o reemplazar la resolución anulada; la declaración del derecho a los perjuicios, cuando se hubieren solicitado, y el envío de los antecedentes al Ministerio Público, cuando estimare que la infracción pudiere ser constitutiva de delito, e

i) Cuando se hubiere dado lugar al reclamo, el interesado podrá presentarse a los tribunales ordinarios de justicia para demandar, conforme a las reglas del juicio sumario, la indemnización de los perjuicios que procedieren y ante el Ministerio Público, la investigación criminal que correspondiere. En ambos casos, no podrá discutirse la ilegalidad ya declarada”.

Esta norma es coincidente con la opinión de la Corte en la medida que permite reclamar ante la Corte de Apelaciones de Santiago o ante la del domicilio del reclamante, a su elección; pues estandariza la tramitación de los contenciosos administrativos, y elimina las

barreras de acceso a la justicia que podrían haberse producido, por ejemplo, con la radicación de la competencia sólo ante la Corte de Santiago. Con ello, se fortalece el principio de regionalización, evitando costos excesivos y el perjuicio del derecho a defensa, tanto del reclamante como del reclamado.

Para la tramitación del reclamo la norma se remite al contenido del artículo 47, que en lo pertinente señala que:

"(…) El reclamo deberá interponerse dentro de los 15 días siguientes a la notificación de la resolución impugnada, según las siguientes reglas:

a) El reclamante señalará en su escrito, con precisión, la resolución objeto del reclamo, la o las normas legales que se suponen infringidas, la forma en que se ha producido la infracción y, cuando procediere, las razones por las cuales el acto le perjudica. Si la reclamación no cumple con estos requisitos, la Corte podrá declararla inadmisible.

b) El titular de datos o el responsable de los mismos, según corresponda, podrá hacerse parte en el respectivo reclamo de conformidad a las normas generales.

c) La Corte podrá decretar orden de no innovar cuando la ejecución del acto impugnado produzca un daño irreparable al recurrente.

d) Recibida la reclamación, la Corte requerirá de informe a la Agencia de Protección de Datos Personales, concediéndole un plazo de diez días al efecto.

e) Evacuado el traslado o teniéndosele por evacuado en rebeldía, la Corte podrá abrir un término de prueba, si así lo estima necesario, el que se regirá por las reglas de los incidentes que contempla el Código de Procedimiento Civil.

f) Vencido el término de prueba, se ordenará traer los autos en relación. La vista de esta causa gozará de preferencia para su inclusión en la tabla.

g) Si la Corte da lugar al reclamo en su sentencia decidirá u ordenará, según sea procedente, la rectificación del acto impugnado y la dictación de la respectiva resolución, según corresponda.

h) Tratándose de reclamaciones en contra de una resolución que resuelve un procedimiento sancionatorio, la Corte podrá confirmar o revocar la resolución impugnada, establecer o desechar la

comisión de la infracción, según corresponda y, mantener, dejar sin efecto o modificar la sanción impuesta al responsable.

i) En todo aquello no regulado por el presente artículo, regirán las normas establecidas en el Código Orgánico de Tribunales y en el Código de Procedimiento Civil, según corresponda".

Octavo: Que si bien en términos generales la norma propuesta se encuentra acorde con la ponencia de la Corte, puede formularse algunas observaciones en pro de la coherencia del sistema que se plantea. Como sucede, por ejemplo, con el concepto de "perjuicio" que utiliza la norma, que genera ambigüedades, en el sentido de producir cuestionamientos como: ¿se requerirá de un perjuicio económico, claramente identificable o bastará con acreditar un perjuicio de cualquier índole? ¿El concepto exigiría entonces, la acreditación de un perjuicio propiamente tal, o se refiere más a una especie de agravio? Esta última alternativa parece más acorde con las disposiciones procedimentales de la reclamación, que exigen identificar "las razones por las cuales el acto le perjudica".

En tal sentido, cabe señalar que respecto a la información que el Estado puede restringir, la Corte Interamericana también se ha pronunciado, señalando una serie de estándares que pueden dar luces sobre el agravio exigible para dar paso a esta reclamación lo cual habrá de tenerse en cuenta al afinar la normativa de que se trata. Así lo ha manifestado en el caso Claude Reyes v. Chile:

"88. El derecho de acceso a la información bajo el control del Estado admite restricciones. Este Tribunal ya se ha pronunciado, en otros casos, sobre las restricciones que se pueden imponer al ejercicio del derecho a la libertad de pensamiento y de expresión.

89. En cuanto a los requisitos que debe cumplir una restricción en esta materia, en primer término deben estar previamente fijadas por ley como medio para asegurar que no queden al arbitrio del poder público. Dichas leyes deben dictarse "por razones de interés general y con el propósito para el cual han sido establecidas" (…)

90. En segundo lugar, la restricción establecida por ley debe responder a un objetivo permitido por la Convención Americana. Al respecto, el artículo 13.2 de la Convención permite que se realicen restricciones necesarias para asegurar "el respeto a los derechos o a la reputación de los demás" o "la protección de la seguridad nacional, el orden público o la salud o la moral públicas".

91. Finalmente, las restricciones que se impongan deben ser necesarias en una sociedad democrática, lo que depende de que estén orientadas a satisfacer un interés público imperativo. Entre varias

opciones para alcanzar ese objetivo, debe escogerse aquélla que restrinja en menor escala el derecho protegido. Es decir, la restricción debe ser proporcional al interés que la justifica y debe ser conducente para alcanzar el logro de ese legítimo objetivo, interfiriendo en la menor medida posible en el efectivo ejercicio del derecho".

Por último, resulta propicio resaltar, en lo que toca a la letra h) del artículo 47 transcrito en el motivo que precede, que convendría aclarar la naturaleza del arbitrio procesal previsto en esa disposición, esto es si corresponde a un recurso o a una acción de lo contencioso administrativo, toda vez que las expresiones que utiliza el Mensaje refieren inequívocamente a un estadio procesal recursivo –una segunda instancia- que no condice con los términos propiamente aplicables a una reclamación por vía de acción, cuyo resolutivo se formula con el acogimiento o rechazo de lo solicitado.

Noveno: Que el artículo 25 de la propuesta, expone una serie de reglas especiales aplicables a las bases de datos compuestas sobre la base de antecedentes personales relativos a infracciones penales, civiles, administrativas y disciplinarias.

El texto completo de este artículo es el siguiente:

"Artículo 25.- Datos relativos a infracciones penales, civiles, administrativas y disciplinarias. Los datos personales relativos a la comisión y sanción de infracciones penales, civiles, administrativas o disciplinarias sólo pueden ser tratados por los organismos públicos para el cumplimiento de sus funciones legales, dentro del ámbito de sus competencias y en los casos expresamente previstos en la ley.

En las comunicaciones o difusión de información que realicen los organismos públicos con ocasión del tratamiento de estos datos personales, deberán velar en todo momento porque la información comunicada o hecha pública sea exacta, suficiente, actual y completa.

No podrán comunicarse o hacerse públicos los datos personales relativos a la comisión y condena de infracciones penales, civiles, administrativas o disciplinarias una vez prescrita la acción penal, civil, administrativa o disciplinaria respectiva o una vez que se haya cumplido o prescrito la pena o la sanción impuesta, lo que deberá ser declarado o constatado por la autoridad pública competente. Lo anterior es sin perjuicio de la incorporación, mantenimiento y consulta de esta información en los registros que llevan los órganos públicos por expresa disposición de la ley, en la forma y por el tiempo previsto en la ley que establece la obligación específica correspondiente. Las personas que se desempeñen en los órganos públicos están obligadas a guardar secreto respecto de esta información, la que deberá ser mantenida como información reservada.

Cuando la ley disponga que la información relativa a la comisión y sanción de infracciones penales, civiles, administrativas y disciplinarias deba hacerse pública a través de su incorporación en un registro de sanciones o su publicación en el sitio web de un órgano público o en cualquier otro medio de comunicación o difusión, sin fijar un período de tiempo durante el cual deba permanecer disponible esta información, se seguirán las siguientes reglas:

a) Respecto de las infracciones penales se aplicarán los mismos plazos establecidos para la eliminación de las anotaciones prontuariales señaladas en el decreto ley N° 409, de 1932 y el decreto N° 64, de 1960, ambos del Ministerio de Justicia.

b) Respecto de las infracciones civiles, administrativas y disciplinarias permanecerán accesibles al público por el período de cinco años.

Exceptúanse de la prohibición de comunicación los casos en que la información sea solicitada por los Tribunales de Justicia u otro organismo público para el cumplimiento de sus funciones legales y dentro del ámbito de su competencia, quienes deben guardar secreto respecto de ella y mantener la debida reserva.”

Décimo: Que, como puede verse, el inciso primero de la disposición transcrita estipula una importante limitación para el tratamiento de esta clase de bases de datos, prohibiendo cualquier procesamiento de las mismas que no se encuentre expresamente previsto en la ley. Esta limitación parece adecuada, en tanto permite proteger el principio de inocencia y precaver posibles discriminaciones arbitrarias o ilegales a los titulares de los datos.

La especial característica de esta información, que permite imponer su restricción al acceso público a ella, hace recomendable una extensión de estas limitaciones, en términos similares o análogos, a la legislación aplicable a entes que no constituyan organismos públicos en el sentido de la ley, especialmente considerando la posibilidad de acceder a algunos de estos datos de manera masiva.

Esta alternativa ya se encuentra cubierta en lo que se refiere al Poder Judicial, según lo preceptuado en el artículo 2 de la ley N° 20.886, que estipula lo siguiente: “Se prohíbe el tratamiento masivo de los datos personales contenidos en el sistema de tramitación electrónica del Poder Judicial, sin su autorización previa. La infracción cometida por entes públicos y privados a lo dispuesto en este inciso será sancionada conforme a la ley N° 19.628.”

La norma del inciso segundo es una emanación del principio de calidad (establecido en el artículo 3 letra d) del proyecto), que señala que “Los datos personales deben ser exactos y, si fuere necesario, completos y actuales, en relación con los fines del tratamiento”.

La disposición contenida en el tercer inciso del artículo 25 propuesto presenta una redacción clara en el sentido de prohibir toda divulgación y comunicación de esta clase de datos, pero cabe recordar que tratándose de acciones o penas cumplidas o prescritas, existen normas que pudieran llevar a que no se aplique la regla propuesta respecto de varias instituciones públicas distintas, tanto por la existencia de la norma del artículo 24 del proyecto, como por la exclusión de esta ley a todo tratamiento de base de datos regido por una ley especial, conforme al artículo 1° de la iniciativa.

Respecto a los tribunales que componen el Poder Judicial, rige plenamente -salvo excepciones legales- el principio de publicidad establecido en el artículo 9° del Código Orgánico de Tribunales, lo que concuerda con la norma del artículo 2° de la ley N° 20.886, que modifica el código de procedimiento civil para establecer la tramitación digital de los procedimientos judiciales, que dispone que:

“Los sistemas informáticos que se utilicen para el registro de los procedimientos judiciales deberán garantizar el pleno acceso de todas las personas a la carpeta electrónica en condiciones de igualdad, salvo las excepciones establecidas por la ley.”

Undécimo: Que el sistema informático del Poder Judicial es un registro que la propia ley mandata, por lo que debe entenderse que le es aplicable la excepción contenida en el inciso segundo del artículo 25 del proyecto en estudio, que expresa: “Lo anterior es sin perjuicio de la incorporación, mantenimiento y consulta de esta información en los registros que llevan los órganos públicos por expresa disposición de la ley, en la forma y por el tiempo previsto en la ley que establece la obligación específica correspondiente”. De tal manera, y también atendida la licitud en el tratamiento de datos personales que realiza el Poder Judicial, en virtud del artículo 57 del proyecto, las restricciones a la comunicación o publicación de datos personales relativos a la comisión y condena de infracciones penales, civiles, administrativas o disciplinarias, una vez prescrita la acción penal, civil, administrativa o disciplinaria respectiva o una vez que se haya cumplido o prescrito la pena o la sanción impuesta, no empecerían al Poder Judicial. En este entendido, las disposiciones legales actualmente vigentes en materia de registro y publicidad, funcionarían de manera coherente y coordinada.

Las facultades de los tribunales, para requerir antecedentes, quedan a salvo con lo dispuesto por el inciso final del artículo 25 en estudio, que expresa: “Exceptúanse de la prohibición de comunicación los casos en que la información sea solicitada por los Tribunales de Justicia u

otro organismo público para el cumplimiento de sus funciones legales y dentro del ámbito de su competencia, quienes deben guardar secreto respecto de ella y mantener la debida reserva". En este caso, sería útil contar con una aclaración de la compatibilidad entre las expresiones "guardar secreto respecto de ella y mantener la debida reserva", y el principio y deber general de publicidad que pesa sobre los tribunales de la República (en términos institucionales, pues a nivel individual, se entiende que siempre rige la regla de la confidencialidad).

Por otra parte, cabe reparar en que, el juego de la regla general (la prohibición de comunicación y publicación de este tipo de información) con las excepciones genera dudas respecto de otros organismos. Así, cabe cuestionarse ¿cómo cabría interpretar esta exclusión respecto de organismos regidos por leyes especiales, y que participan en la investigación, persecución, enjuiciamiento y sanción de infracciones administrativas? Respecto de este último cuestionamiento, los incisos 4° y 5° de la propuesta pueden entregar algunas razones fuertes para considerar que la excepción del artículo 24 en relación a los datos relativos "a la investigación, persecución, enjuiciamiento o sanción de infracciones penales, civiles y administrativas" no debiese aplicarse una vez que la sanción en cuestión ha sido efectivamente cursada, cobrando plena aplicación lo dispuesto en el inciso 3°, debiendo el respectivo órgano público quitar la publicidad relativa a la misma. Sin embargo esta cuestión no es de suyo evidente, y podría clarificarse para evitar dudas interpretativas.

Los incisos 4° y 5° de este artículo 25 tienen la loable pretensión de evitar la existencia de discriminaciones arbitrarias o la extensión artificial e ilegítima de condenas sociales, pero pueden implicar algunas importantes dificultades operativas. Por una parte, porque los plazos a los que se refiere el Decreto Ley N° 409 no operan por el sólo ministerio de la ley y requieren la realización de conductas específicas por parte del condenado (mantenerse bajo la supervisión, o en contacto con el Patronato de Reos o su continuador); y por otra, porque el Decreto Ley N° 409 y el Decreto N° 64, dan cuenta de plazos distintos para eliminar las anotaciones a que hacen referencia, todo lo que derivará en interpretaciones jurídicas que podrían anticiparse.

Lo anterior, porque probablemente estas circunstancias no sean fácilmente automatizables, lo que a su vez puede provocar la destinación de recursos especiales o, inclusive, una sobrecarga de trabajo completamente innecesaria. En este sentido, parece recomendable, o especificar plazos simples para cada una de estas decisiones, o la utilización de diseños como el adoptado por la ley de tramitación electrónica, consistente en permitir la consulta de aquellos documentos públicos que establecen sanciones, prohibiendo su tratamiento masivo, o potencialmente discriminatorio, a través de la tipificación de sanciones especiales, particularmente disuasivas;

Duodécimo: Que el artículo 47 se refiere a la “Reclamación judicial”, estableciendo el derecho al recurso en los siguientes términos:

Reclamación judicial. Las personas naturales o jurídicas que se vean afectadas por una resolución final o de término de la Agencia de Protección de Datos Personales podrán deducir un reclamo de ilegalidad ante la Corte de Apelaciones de Santiago o la del lugar donde se encuentre domiciliado el reclamante, a elección de este último.. El reclamo deberá interponerse dentro de los 15 días siguientes a la notificación de la resolución impugnada, según las siguientes reglas”.

Las reglas de procedimiento fueron transcritas en el numeral 15, a propósito de los comentarios relativos al artículo 23.

Como ya se dijo anteriormente, esta norma se refiere al procedimiento de reclamación judicial que pueden iniciar aquellas personas que se vean afectadas por una resolución final o de término de la Agencia de Protección de Datos Personales. Si bien este procedimiento se regula en extenso en esta norma, a través de otras disposiciones se hace aplicable también respecto de otros actos administrativos, como los referidos en el artículo 23 inciso 3° (Ejercicio de los derechos del titular y reclamo de ilegalidad), en el 45 letra h (Procedimiento administrativo de tutela de derechos) y en el 46 en el letra k (Procedimiento administrativo por infracción de ley).

Al respecto, cabe reiterar las observaciones realizadas en el motivo octavo con la salvedad que si bien, por regla general, todo acto de la Administración se encuentra sujeto al control de los tribunales de justicia, en tanto su misión es cautelar la vigencia de los derechos de las personas y, en consecuencia, la mantención del Estado de Derecho, esa impugnabilidad encuentra limitación en la existencia de recursos previos contra los actos en actual tramitación a través de la vía administrativa. Los preceptos bajo análisis, en tanto permiten la judicialización sólo de los actos que han sido previamente reclamados ante la Administración (es decir, exige el agotamiento de la vía administrativa), sólo harían posible dicha reclamación en los casos en que la autoridad hubiere rechazado la impugnación administrativa. Esta hipótesis restringe la posibilidad de los particulares de reclamar directamente ante los tribunales, respecto de las resoluciones dictadas por la autoridad en cumplimiento de la ley, limitando el ámbito del control judicial;

Decimotercero: Que, finalmente, el artículo 51 de la propuesta estipula el estatuto aplicable en relación a los posibles casos de responsabilidad civil a que podría dar lugar la infracción de los derechos, normas y principios regulados en la iniciativa legal. Su texto es el siguiente:

“Artículo 51.- Norma general. El responsable de datos deberá indemnizar el daño patrimonial y moral que cause al o los titulares, cuando en sus operaciones de tratamiento de datos infrinja los principios y obligaciones establecidos en esta ley y les cause daño, sin perjuicio de los demás derechos que concede esta ley al o los titulares de datos.

La acción indemnizatoria señalada en el inciso anterior podrá interponerse una vez ejecutoriada la resolución que resolvió favorablemente el reclamo interpuesto ante la Agencia de Protección de Datos Personales o la sentencia se encuentre firme y ejecutoriada, en caso de haber presentado un reclamo judicial, y se tramitará de conformidad a las normas generales del Código de Procedimiento Civil.”

En primer inciso de este artículo no parece ofrecer mayores dificultades. No así el inciso segundo, cuya norma presenta a lo menos dos situaciones posibles de observar. Por una parte, omite regular aquellos casos en que se produzcan hipótesis de responsabilidad civil sin responsabilidad administrativa, es decir, que las personas podrían acceder directamente a la vía judicial, sin necesidad del reclamo administrativo; y por otra, asumiendo la postura de la Corte frente a los procedimientos contenciosos administrativos especiales, la exigibilidad de la indemnización debiera seguir la regla contemplada por el literal i) del artículo 151 de la Ley de Municipalidades, que dispone que “Cuando se hubiere dado lugar al reclamo, el interesado podrá presentarse a los tribunales ordinarios de justicia para demandar, conforme a las reglas del juicio sumario, la indemnización de los perjuicios que procedieren y ante el Ministerio Público, la investigación criminal que correspondiere. En ambos casos, no podrá discutirse la ilegalidad ya declarada”. De este modo se incentivaría el uso de esta acción, ahorrando los costos que implica un juicio ordinario, y evitando posibles dilaciones injustas para el titular.

Decimocuarto: Que fuera de los artículos consultados, cabe hacer referencia a algunas disposiciones que, no obstante no haberlo sido en el oficio respectivo, podrían afectar las atribuciones y facultades de los tribunales de justicia, en los términos del artículo 77 de la Constitución Política de la República y 16 de la Ley N° 18.918, Orgánica Constitucional del Congreso Nacional.

Resulta relativamente evidente que toda la eficacia de la propuesta normativa actualmente en análisis se construye sobre la base del concepto de “dato personal”. En este sentido, serán los contornos de este concepto aquellos que definan, con rigor, tanto el alcance y la amplitud de los derechos del titular, así como –por extensión– los márgenes de las atribuciones de los tribunales y la Agencia para su resguardo.

En concreto, la propuesta opta por una definición que disminuye radicalmente el rango de aplicación de la definición vigente, en la medida que excluye del carácter de “dato personal”, a aquellos datos de personas que no son identificables a través de “medios razonablemente utilizados”.

Esta nueva definición propuesta parece ambigua por dos razones. Primero, porque no especifica claramente qué es aquello que podría constituir la razonabilidad del medio empleado para relacionar un dato específico de una base de datos con una persona. ¿Se refiere a la razonabilidad del esfuerzo o el trabajo empleado?, ¿se refiere al tiempo de cómputo que implica el medio de identificación? o ¿se refiere a la imposibilidad de realizar la identificación mediante medios automatizados? Segundo, porque al adoptar este nuevo criterio -y asumiendo que es posible aislar un concepto de razonabilidad del medio que resulte jurídicamente operativo-, la definición propuesta amenaza con disminuir los estándares de protección actualmente vigentes, incentivando la generación de espacios (resquicios) en los que podría darse un tratamiento abusivo de datos, en tanto no cabrían en la definición de dato personal propuesta por la ley. Ello, en la medida que el responsable del tratamiento demuestre que el medio que empleó para identificar al titular del dato fue arduo, difícil u oneroso y, por lo tanto, a través de un medio que no responda al concepto de “razonablemente utilizado”;

Decimoquinto: Que estas consideraciones, que pueden ser extensivas a la definición de “proceso de anonimización o disociación” que prevé la letra k) del artículo 2 de la propuesta, sumadas al interés que debe pesar sobre los poderes del Estado en minimizar los resquicios legales, son suficientes para justificar la mantención de la definición actualmente vigente, asegurando que las disposiciones de la ley en cuestión sean aplicables para la mayor cantidad de casos posibles.

Empleo de bases de datos que cuenten con datos personales sensibles en investigaciones y procedimientos judiciales. En la propuesta normativa queda suficientemente clara la potestad de los diversos organismos que contribuyen a la investigación y persecución de responsabilidades penales, civiles y administrativas, en relación al tratamiento de datos personales y sensibles.

En este sentido, el proyecto carece de una consideración general que especifique que fuera de las condiciones estipuladas en el artículo 16 de la propuesta- el consentimiento del titular de los datos puede ser reemplazado por una autorización judicial, para su obtención o tratamiento, en una manera similar a la que en materia penal prevé el artículo 9° del Código Procesal Penal. Lo anterior, resulta especialmente crítico si se considera el régimen de exclusión de prueba vigente en nuestro sistema penal, y la manera en que se construyen las

excepciones que establece el artículo 24 de la propuesta respecto del tratamiento de datos personales para la investigación, persecución, enjuiciamiento o sanción de infracciones penales, civiles y administrativas, particularmente en contextos excepcionales, como los datos secretos o confidenciales;

Decimosexto: Que si bien no viene consultado, esta Corte observa que un aspecto claramente orgánico constitucional del proyecto se encuentra en el Título VIII que aborda el Tratamiento de los Datos Personales por el Congreso Nacional, el Poder Judicial y organismos públicos dotados de autonomía constitucional.

En efecto, por una parte se expresa que las disposiciones del proyecto no importan una afectación del trabajo del Poder Judicial en la materia a legislar, puesto que se considera lícito el tratamiento de los datos personales que efectúan los tribunales para el cumplimiento de sus funciones jurisdiccionales, dentro del ámbito de su competencia. Por otro lado, la iniciativa permite que las autoridades ya mencionadas –entre ellas el Poder Judicial- dicten las normas e instrucciones necesarias para dar cumplimiento a los principios y obligaciones en materia de protección de datos personales, sin la fiscalización ni supervisión de la institucionalidad que se crea para controlar dicho ámbito –la Agencia de Protección de Datos Personales-, circunstancias que se estiman beneficiosas.

Además, en el inciso segundo del artículo 58 del proyecto se establece una acción especial de reclamación respecto de estas autoridades, excluyendo al Poder Judicial, dado que conocerá de ella por medio de las Cortes de Apelaciones, vale decir, se asigna un rol de autonomía relativa al Poder Judicial y se otorga una acción judicial en la materia, regulación que también se considera adecuada.

Por estas consideraciones y de conformidad, además, con lo dispuesto en los artículos 77 de la Constitución Política de la República y 18 de la Ley N° 18.918, Orgánica Constitucional del Congreso Nacional, se acuerda informar en los términos precedentemente expresados el proyecto de ley que protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales.

- - -

DISCUSIÓN EN GENERAL

1.-Exposiciones escuchadas por la Comisión

Como se ha señalado precedentemente la Comisión estimó pertinente, antes de pronunciarse en general sobre las

iniciativas en informe, recibir la opinión de distintas personas y entidades interesadas en dar a conocer sus puntos de vista respecto de los proyectos de ley que se refunden en este informe.

Al iniciarse la consideración de este asunto, **el Presidente de la Comisión, Honorable Senador señor Felipe Harboe**, ofreció el uso de la palabra **al Ministro de Hacienda, señor Rodrigo Valdés**, quien agradeció la invitación de la Comisión para el estudio de estas iniciativas de ley.

Seguidamente, manifestó que estamos ante iniciativas de gran relevancia que intentan avanzar, actualizar y modernizar el marco normativo e institucional vigente en Chile para el tratamiento de los datos personales. Agregó que el proyecto de ley del Ejecutivo busca equilibrar la protección y la libre circulación de la información.

Expuso que los cambios tecnológicos han modificado sustancialmente la importancia de la protección de los datos personales. Reseñó que hace quince años la cantidad de datos era muy menor en comparación con el actual.

Expresó que el proyecto de ley busca dotar al país de una legislación moderna y flexible en materia de tratamiento de datos personales, que sea consistente con los compromisos internacionales adquiridos luego de su incorporación a la OCDE y ajustada a las normas y estándares internacionales en la sociedad de la información.

En seguida, sostuvo que estamos ante la última iniciativa de la llamada agenda de probidad y transparencia a la que se comprometió el actual Gobierno. Informó que el Subsecretario de Hacienda, señor Alejandro Micco será el representante del Ministerio de Hacienda en la tramitación del presente proyecto de ley.

Concluyó su intervención, señalando que es la segunda iniciativa que ingresa al Congreso Nacional con un informe de productividad. Constató que hubo un instructivo presidencial en que se dispone que los proyectos de ley que firmen los miembros del Comité Económico de Ministros deben ir acompañados del mencionado informe.

El Honorable Senador señor Larraín hizo presente que junto a los Honorables Senadores señores Harboe, Araya, Lagos, y Tuma presentó un proyecto de reforma constitucional, que consagra el derecho a la protección de los datos personales. La mencionada iniciativa fue aprobada en el Senado y se encuentra actualmente en la Cámara de Diputados.

Consignó que era conveniente que la Constitución Política de la República consagre el derecho a la protección de datos personales. Le solicitó al señor Ministro que el Poder Ejecutivo le otorgue urgencia al mencionado proyecto de ley.

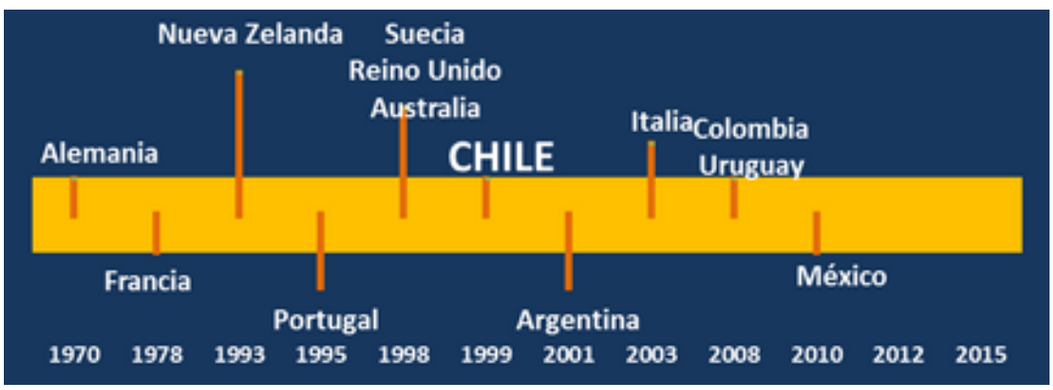
A continuación, **el Presidente de la Comisión, Honorable Senador señor Harboe** ofreció la palabra al Subsecretario de Hacienda, señor Alejandro Micco.

El Subsecretario del Ministerio de Hacienda, señor Alejandro Micco agradeció la invitación de la Comisión de Constitución, Legislación, Justicia y Reglamento a participar en el estudio de este proyecto de ley.

Señaló que en Chile se encuentra vigente la ley N° 19.628 sobre Protección de la Vida Privada. Agregó que en el mencionado cuerpo legal se establece un conjunto de normas que regulan el tratamiento y la protección de los datos personales.

Seguidamente, reseñó que en el año 1999 Chile fue uno de los países pioneros en introducir este tipo de regulación que protege los datos personales. Puntualizó que nuestro país fue el primero en Latinoamérica en darse un marco regulatorio en esta área.

Luego, hizo presente que, con posterioridad, una serie de países latinoamericanos han hecho cambios regulatorios en esta materia, tales como Argentina, Colombia, Uruguay y México. Lo anterior se ve reflejado en el siguiente cuadro.



Admitió que las condiciones que existían cuando se publicó la ley antes mencionada son muy distintas al actual escenario de la economía, por lo tanto, aseveró que se hace imperiosa una modernización en la presente materia.

Por ejemplo, recordó que en el año 2000 en Chile no había ningún teléfono *Smartphone* y que en el año 2015 ya contábamos con 7,9 millones de estos aparatos.

Hizo presente que en el año 2000 no se realizaban ventas en línea, y el 2015, éstas crecieron a una tasa del 29,7%. En cuanto al acceso a internet en los hogares, éste se incrementó de un 8,7% el año 2000 a un 66,5% el año 2015. Todo lo anterior se ve reflejado en el siguiente cuadro.

Cuadro comparativo con estadísticas 2000-2015

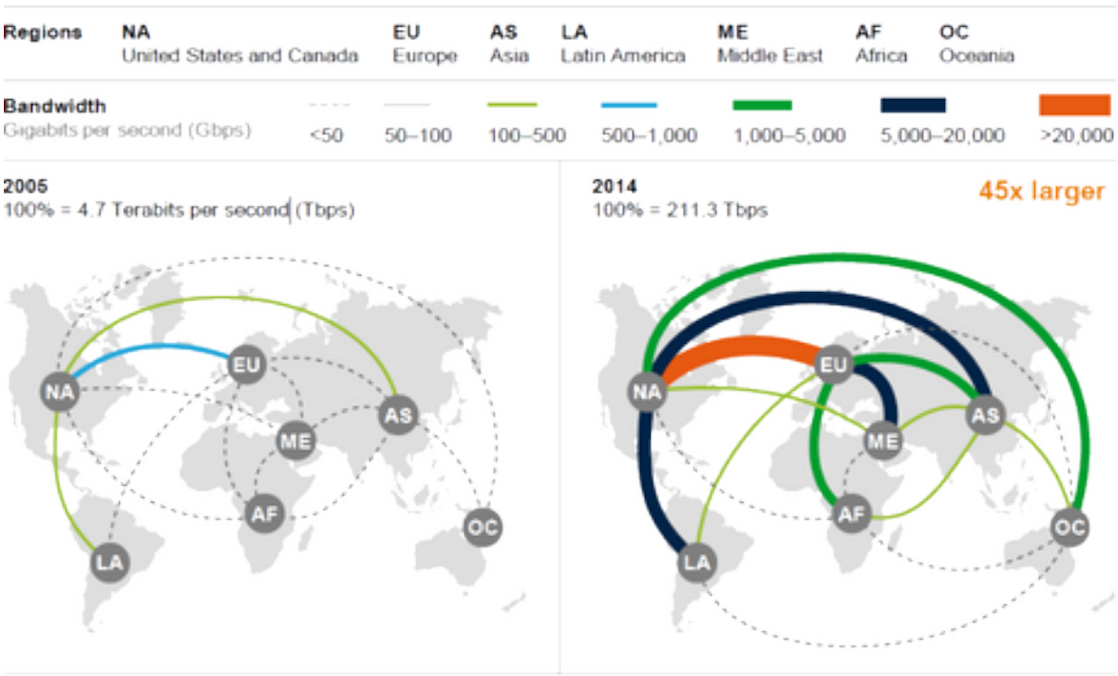
	2000	2015
Teléfonos *smartphones*	0	7,9 millones
Aumento anual ventas en línea	0%	29,7%
Acceso a internet (hogares)	8,7%	66,5%
Suscripción Banda Ancha	0%	15,64%
Dispositivo almacenamiento	*Disquette* (4,1 Mb)	Disco Duro (2 Tb)

Añadió que también las capacidades de almacenamiento han aumentado considerablemente, pasando de 3 Mb a una de características ilimitadas en la nube.

Manifestó que mediante el *Big Data* se logra procesar una infinidad de datos que facilitan la oferta de productos a la población. Añadió que otro tema nuevo en materia de datos que se está aplicando en Chile lo constituye la información genética.

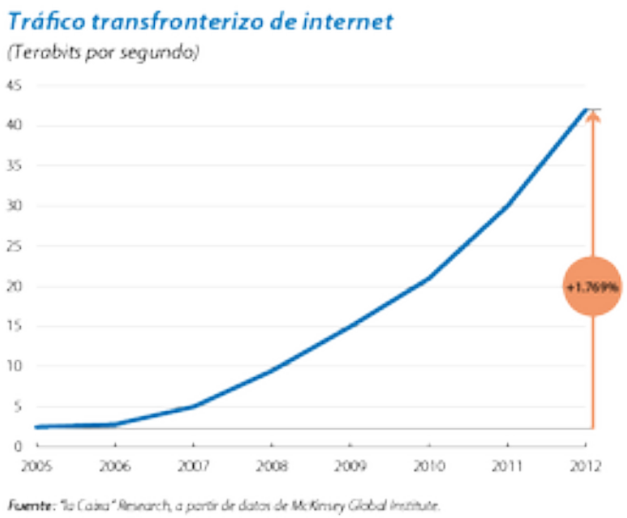
En seguida, y en relación al contexto mundial, señaló que los flujos de información han cambiado en forma sideral entre el año 2005 y el 2014. Ello se refleja en el siguiente cuadro:

Flujos de datos globales.
Flujo de *gigabits* por segundo. Estudio *McKinsey Global Institute*.



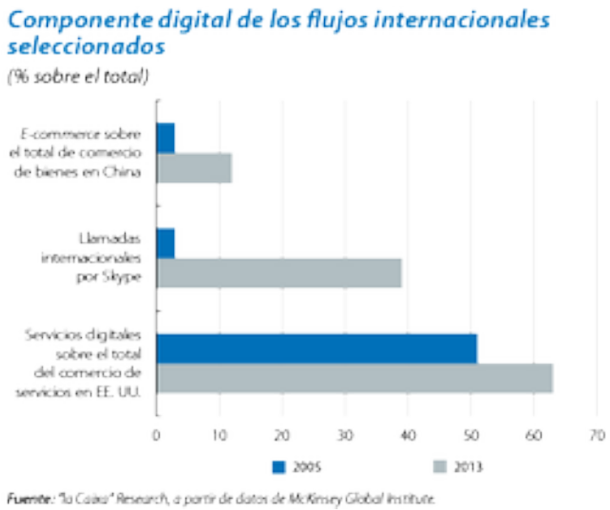
Explicó que el ancho de las líneas representa la cantidad de datos que se movilizan por segundo. Enfatizó que todo lo anterior lleva necesariamente a readecuar nuestra legislación.

En cuanto al tráfico transfronterizo entre el año 2005 y 2012 hubo un crecimiento de más de 1.700%. Ello se refleja en siguiente cuadro:



Fuente: "la Caixa" Research, a partir de datos de McKinsey Global Institute.

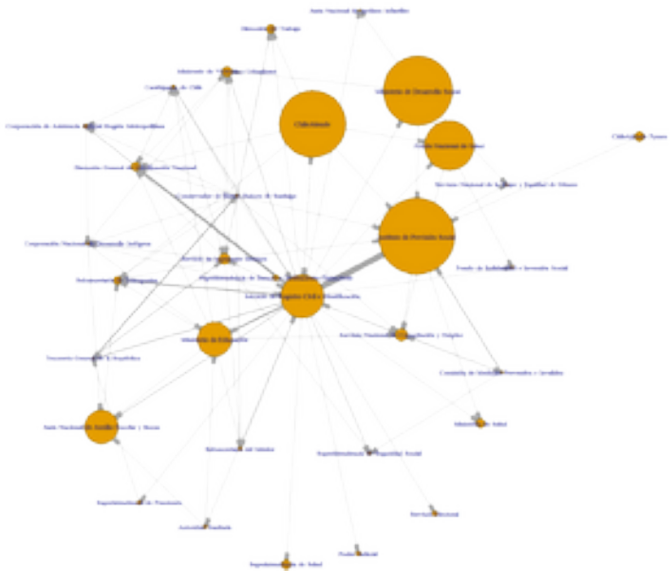
Consignó que también se ha incrementado exponencialmente el desarrollo de la industria del *E-commerce*, lo que se ve reflejado en el esquema que a continuación se detalla:



Añadió que los servicios al ciudadano hoy requieren interacción digital entre las instituciones públicas y privadas. Ello demanda un marco robusto de protección de datos personales según el estudio "*Network Analysis for Chile Atiende*" del MIT.

Connotó que, según dicho estudio, el Instituto de Previsión Social (agencia con más visitas web al año, alrededor de 4.200 al día, 1.500.000 al año), tiene su interacción más fuerte con el Registro Civil, que a la vez es el nódulo con más interconexiones con otros servicios.

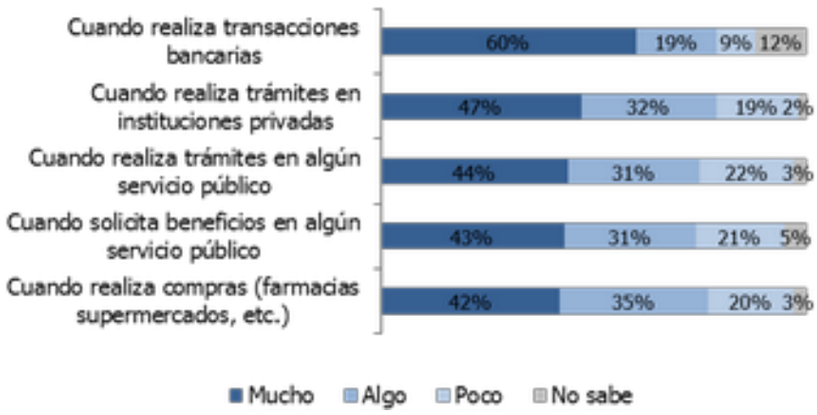
Destacó que en el siguiente gráfico se ve reflejado lo anterior:



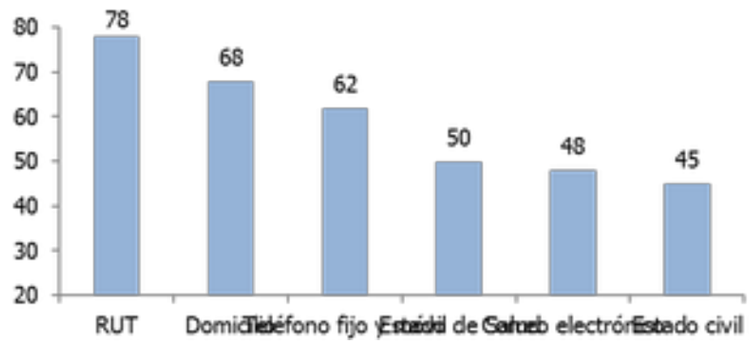
Apuntó que cualquier ley de datos personales tiene que considerar que uno de los principales usuarios de éstos es el Estado.

Luego, destacó que dado el uso de tecnologías para trámites, transacciones bancarias, perfiles virtuales, entre otros, las personas tienen entre sus preocupaciones el cuidado de su información personal. Así lo demuestra el siguiente gráfico.

Situaciones en las cuales las personas se preocupan de su información personal, 2014



Porcentaje de personas que cuida distintos tipos de información personal, 2014

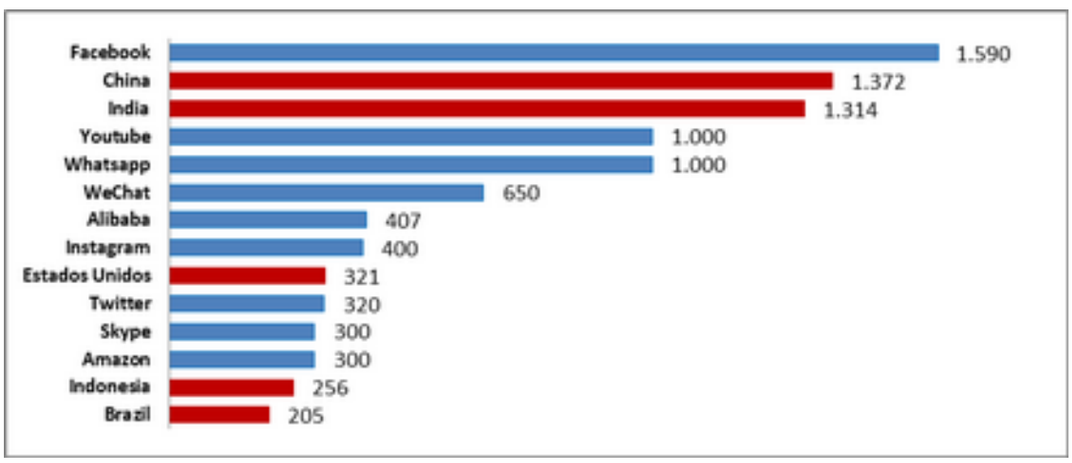


A continuación, hizo presente que el desarrollo de la tecnología a nivel mundial y en Chile ha llevado a que surja una industria y una economía digital de gran transcendencia en el manejo y procesamiento de datos, tanto en el sector público como en el privado.

Recalcó que estamos frente a una iniciativa relevante tanto por las preocupaciones y bienestar de las personas, como para el desarrollo de la economía digital en nuestro país.

Abogó por contar con un marco regulatorio que permita el uso pero no el abuso de los datos de las personas. Agregó que las plataformas web más utilizadas, llegan a tener un nivel de usuarios similar a la población de los países más grandes del mundo y se espera que el traspaso de información entre países siga creciendo exponencialmente según el Instituto de análisis de McKinsey.

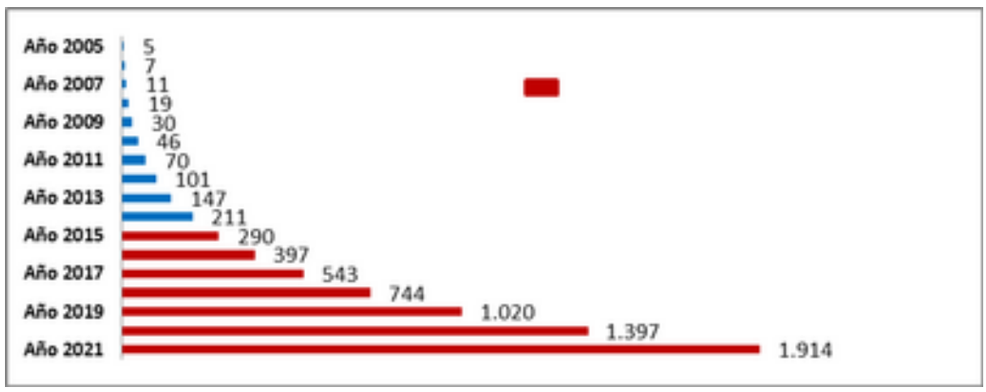
Ello se ve reflejado en el siguiente gráfico:



Aseveró que Facebook tiene más usuarios que los habitantes de China y que India.

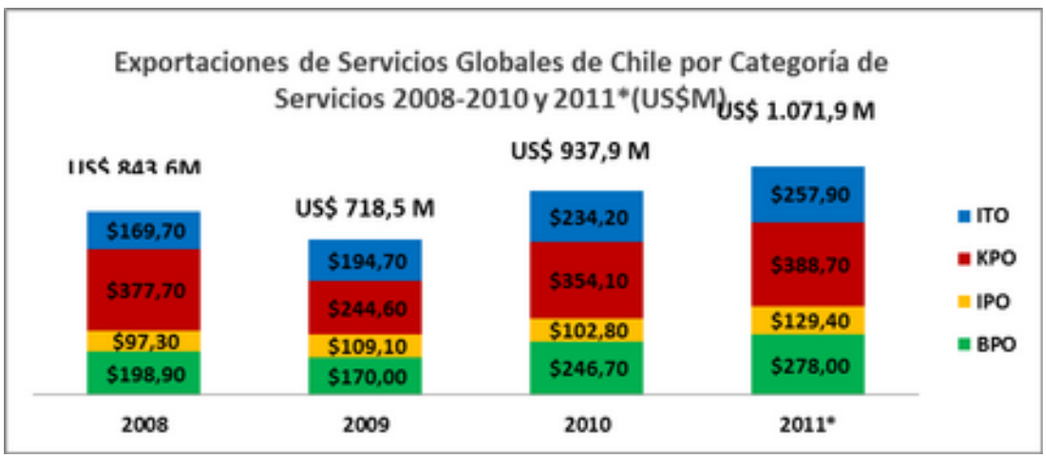
Reiteró que estamos ante una nueva realidad de la que hay que hacerse cargo.

Manifestó que el cuadro siguiente hace referencia al uso de ancho de banda transfronterizo (Terabits por segundo)



Consignó que la economía chilena también ha evolucionado positivamente en la exportación de Servicios Globales al mundo.

Exportaciones de Servicios Globales de Chile por Categoría de Servicios 2008-2010 y 2011*(US$M)



ITO
Tecnología de Información
Aplicaciones
- Soporte técnico remoto
- Desarrollos web

Infraestructura y sistemas
- Manejo ciclo de vida de computadores
- Captura y procesamiento de datos

KPO
Procesos de negocios complejos
- Servicios financieros
- Investigación y análisis de mercado
- Servicios legales
- Diseño y servicios de ingeniería
- Investigación farmacéutica

IPO
Procesos de Innovación

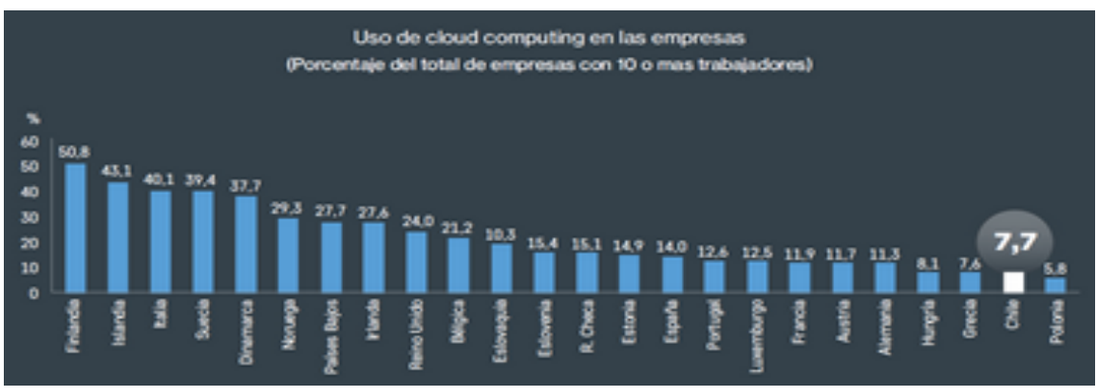
BPO
Procesos de negocios
- Centro de contacto
- Contabilidad, finanzas y servicios de pago
- Recursos humanos

A modo de ejemplo, señaló que la exportación de servicios que no están relacionados con el turismo o con el transporte creció en Chile desde niveles de US$800M a US$4.000M el año 2016, por lo tanto, añadió, se transforma en una industria más importante que la de los salmones.

Seguidamente, hizo presente que exportamos servicios, incluidos Servicios Globales a más de 10 países del mundo. Rubro que solo ha crecido en los últimos años y donde tenemos ventajas comparativas.

Precisó que Chile tiene una ventaja comparativa muy interesante, que es la de estar en el mismo huso horario que Estados Unidos de Norteamérica, lo que permite la exportación de servicios, entre ellos el de manejo de datos.

En relación al desarrollo de la economía digital, subrayó que el 7,7% de las empresas del país, con más de 10 trabajadores, usan *cloud computing*. Lo anterior se detalla a continuación.



Luego, observó que tanto de la experiencia comparada como de las recomendaciones de la OCDE a Chile, se desprende que nuestro país no cuenta con un organismo que supervise el correcto tratamiento y protección de los datos personales.

Agregó que tanto el informe del Consejo para la Transparencia, como el de la Corte Suprema sobre el último proyecto de ley de protección de datos personales coinciden en la falta de una nueva institucionalidad.

Sostuvo que en la evaluación de la ley N° 19.628 sobre Protección de la Vida Privada de la Cámara de Diputados, se concluye que la legislación chilena requiere de una autoridad administrativa de control independiente.

En esta materia, expresó que a nivel mundial existe una serie de formas que adopta la institucionalidad para la protección de los datos. Consignó que la tendencia a nivel mundial consiste en contar con una institucionalidad exclusiva, separada de la de la transparencia.

Aseveró que es necesario analizar cómo interactúa el derecho de proteger los datos personales con la transparencia. Se preguntó si éstas debían estar bajo el alero de distintos organismos.

Constató que la mayoría de los países cuentan con instituciones que funcionan de manera independiente. Para ello, puntualizó, hay diversas razones, una de ellas es que estamos frente a dos derechos que pueden ser contradictorios.

Lo anterior, explicó, motivó la separación de ambas institucionalidades en el presente proyecto de ley. Agregó que en la iniciativa se crea la Agencia de Protección de Datos Personales, la que gozará de cierto nivel de autonomía.

Asimismo, afirmó que se crea un régimen general de cumplimiento de la ley que tiene un procedimiento administrativo por infracción a la ley. Manifestó que éste se puede iniciar a petición de parte o de oficio. Posterior a ello, la Agencia presentará la formulación de cargos contra el responsable de los datos y este último tiene diez días de plazo para presentar los descargos. En caso de que existan hechos sustanciales, pertinentes y controvertidos se abre un término probatorio de siete días. Agregó que la Agencia deberá pronunciarse sobre cada uno de los aspectos conocidos en el expediente y frente a esa resolución se puede interponer recurso de reposición dentro del plazo de cinco días.

Detalló que de la resolución de la Agencia se podrá presentar una reclamación judicial. Señaló que la persona natural o jurídica que se vea afectada por una resolución final de la Agencia de Protección de Datos Personales podrá deducir un reclamo de ilegalidad a la Corte de Apelaciones respectiva. La Corte requerirá informe a la Agencia, concediéndole un plazo de diez días y el mencionado tribunal podrá abrir un término probatorio si lo considera necesario. Añadió que vencido este plazo se ordenará traer los autos en relación. Subrayó que la vista de esta causa gozará de preferencia. Recalcó que la Corte puede confirmar la decisión de la Agencia u ordenar que ésta rectifique su resolución.

Señaló que para fijar las sanciones se realizó el siguiente estudio comparado:

País	Sanciones
Argentina	Sanción no monetarias: • Advertencias, suspensión del derecho de tener una base de dato, cancelación de la base de datos Sanción monetaria: • US$ 64 a US$ 6.400
Chile (PDL actual)	Sanción monetaria: • Infracción leve desde US$ 70 a US$ 3500, • Infracción grave US$ 3.501 a US$ 35.000, • Infracción muy grave US$ 35.001 a US$ 352.000
Uruguay	Sanciones no monetarias: • Advertencias, suspensión de la base de datos por 5 días, cancelación de la base de datos. Sanción monetaria: • 0 a US$ 60.000
España	Esencialmente sanciones monetarias: • Infracción leves: US$ 970 a US$ 43.000 • Infracción graves: US$ 43.001 a US$ 323.000 • Infracción muy graves: US$323.001 a US$ 650.000

Francia	Sanciones no monetarias: • Advertencias y notificaciones Sanciones monetarias: • Primera falta: Hasta US$ 162.000 • Segunda falta en los próximos 5 años: Hasta US$ 356.000 • Además ante la reiteración de faltas, se le ordena a la empresa cesar inmediatamente al tratamiento de datos
Alemania	Esencialmente sanciones monetarias: • Sanción hasta US$356.000 por violación a la ley Además, en caso que la infracción haya tenido un directo beneficio económico, puede llegar a 2 años de cárcel o sancionar por las utilidades que haya generado la violación a la ley.

En esta materia, aclaró que las sanciones deben ser proporcionales. Por lo anterior, explicó que ellas se clasifican el leves, graves y muy graves. Consignó que se debe tener en consideración el volumen de datos tratados y de la sensibilidad de los mismos.

En relación a los principios rectores de la iniciativa en estudio, señaló que son los siguientes:

1.- Principio de licitud de tratamiento. Explicó que para que el tratamiento de un dato personal sea lícito requiere del consentimiento de la persona o que una ley así lo disponga.

2.- Principio de finalidad. Señaló que cuando se solicita un dato, se debe mencionar el uso que se le dará.

3.- Principio de proporcionalidad. Advirtió que lo que se pide debe ser acorde a su finalidad.

4.- Principio de calidad. Aseveró que los datos personales deben ser exactos y, si fuera necesario, completos y actuales, en relación con los fines del tratamiento.

5.- Principio de responsabilidad. Precisó que quienes realicen tratamiento de los datos personales serán legalmente responsables del cumplimiento de los principios, obligaciones y deberes de conformidad a esta ley.

6.- Principio de seguridad. Sostuvo que en el tratamiento de los datos personales se deben garantizar niveles adecuados de seguridad, protegiéndolos contra el tratamiento no autorizado, pérdida, filtración, destrucción o daño accidental y aplicando medidas técnicas u organizativas apropiadas.

7.- Principio de información. Connotó que las prácticas y políticas sobre el tratamiento de los datos personales deben estar permanentemente accesibles y a disposición de cualquier interesado de manera precisa, clara, inequívoca y gratuita.

Agregó que en la legislación comparada los derechos ARCO, a saber, acceso, rectificación, cancelación y oposición, tienen el siguiente contexto:

Derechos ARCO en la legislación comparada

País	Institucionalidad	Acceso	Rectificación	Cancelación	Oposición	Organismos Públicos	Tratamiento Automatizado	Certificación (Compliance)
Argentina	Si	Si	Si	Si	Si	Si	Si	No
Colombia	No	Si	Si	Si	Si	Si	Si	No
México	Si	Si	Si	Si	Si	Si	No	No
Uruguay	Si	Si	Si	Si	Si	Si	Si	No
Estados Unidos	No	Si	Si	Si	Si	Si	Si	Si
Reino Unido	Si	Si	Si	Si	Si	Si	Si	No
Australia	Si	Si	Si	No	Si	Si	No	No
Nueva Zelanda	Si	Si	Si	Si	Si	Si	Si	No
España	Si	Si	Si	Si	Si	Si	Si	No
Francia	Si	Si	Si	Si	Si	Si	Si	No
Alemania	No	Si	Si	Si	Si	Si	Si	No
Portugal	Si	Si	Si	Si	Si	Si	Si	No
Italia	Si	Si	Si	Si	Si	Si	Si	No
Suecia	Si	Si	Si	Si	Si	Si	Si	No

En cuanto a los objetivos del proyecto de ley, enumeró los siguientes:

1.- Establecer las condiciones regulatorias que permitan reforzar los derechos de los titulares de datos personales.

2.- Dotar al país de una legislación moderna y flexible en esta materia, consistente con los compromisos internacionales, especialmente aquellos adquiridos con el ingreso a la OCDE.

3.- Incrementar los estándares legales de Chile en el tratamiento de datos personales para transformarlo en un país con niveles adecuados de protección y seguridad.

4.- Definir estándares regulatorios y condiciones para legitimar el tratamiento de datos personales por parte de los órganos públicos y privados, compatibilizando el cumplimiento de la función pública y los derechos de los ciudadanos.

5.- Contar con una autoridad de control de carácter técnico y una institucionalidad pública que asuma los desafíos regulatorios y de fiscalización en materia de protección de las personas y el tratamiento de los datos personales.

Como conclusión a lo ya expresado, manifestó que el actual marco regulatorio es insuficiente frente a los cambios tecnológicos, económicos y culturales de las últimas décadas; falta una autoridad de control que vele por la correcta aplicación de la ley y debe cumplirse con los compromisos adquiridos internacionalmente.

Enfatizó que existen tres principios fundamentales que deben ser cautelados, a saber: la transparencia, la libre circulación de la información y la protección de la vida privada.

Concluyó su intervención haciendo referencia al informe financiero. Consignó que la iniciativa se estima tendrá un mayor gasto fiscal en régimen de $ 1.428.876 miles, a partir del segundo año de vigencia de la ley, asociado a la creación de la Agencia de Protección de Datos Personales.

Agregó que el mayor gasto fiscal durante el primer año de vigencia de la ley se financiará con cargo a reasignaciones de la Partida Ministerio de Hacienda, en los años siguientes estará considerado en las leyes de presupuestos.

Connotó que la distribución del gasto se grafica de la siguiente manera:

Conceptos/Años	Año 1 (Miles $ 2017)	Año 2 y en régimen (Miles $ 2017)
Remuneraciones	711.401	1.166.196
Gasto corriente	169.057	262.680
Inversión inicial	417.560	-
Total Gastos	1.298.018	1.428.876

A continuación, **el Presidente de la Comisión, Honorable Senador señor Harboe,** ofreció la palabra a los demás integrantes de la Comisión.

El Honorable Senador señor Larraín agradeció el trabajo realizado por el Gobierno. Asimismo, señaló que el proyecto era esperado desde hace mucho tiempo.

Expresó que actualmente tanto el marco regulatorio como la supervisión y control de los datos personales son débiles. Agregó que la situación de los mismos es precaria en comparación con el incremento del acceso a la información y transparencia pública. Recalcó que lo anterior ha debilitado la situación de los datos personales.

Declaró que es muy importante lograr un equilibrio en esta materia. Constató que muchas personas se sienten avasalladas por la cantidad de información que se les solicita.

Por otra parte, consignó que a través de la información pública se está invadiendo la privacidad de muchos individuos. Subrayó que la pregunta que surge es dónde empieza una y termina la otra, dónde fijamos las diferencias, los equilibrios y las simetrías que son necesarias.

Sostuvo que la discusión central del proyecto de ley es la que se refiere a la naturaleza jurídica de la Agencia, en cuanto a la forma de vincularse con la transparencia; la necesidad de que sea exclusiva y la naturaleza de su dependencia.

Luego, añadió que respecto a la relación entre la transparencia y el acceso a la información pública, la separación no debe ser absoluta, porque hay vasos comunicantes entre ambos ámbitos. Aseveró que podría entender la resolución apartada de los conflictos que origina la transparencia versus los que crea la protección de datos personales. Recalcó que la vinculación de los dos temas planteados no se debiera hacer de manera total.

Asimismo, precisó que cuando se resuelve una reclamación en el Consejo para la Transparencia se está tomando una definición de la línea divisoria entre lo público y lo privado.

Se preguntó cuál es el límite que debe existir entre una información privada y la necesidad de que ella adopte el carácter de pública. Ejemplificó con el caso de una persona que padezca una enfermedad infecciosa.

Constató que también, desde el punto de vista de la protección de datos se dan ciertos conflictos respecto a la delimitación de los determinados campos.

En seguida, recordó que presentó un proyecto de ley que busca obligar a que ciertas instituciones en el ámbito privado, tales como federaciones gremiales, confederaciones, etcétera, entreguen información sobre su funcionamiento e integrantes, porque las actividades que ellas desarrollan son de interés público.

Recalcó que en Canadá existe una sola institución que opera por ramas separadas con un nivel de coordinación que permite equilibrar y armonizar la jurisprudencia. Por lo anterior, consideró relevante estudiar la separación total que se plantea en la presente iniciativa.

En relación a la dependencia o autonomía, advirtió que tiene una diferencia sustancial con el proyecto de ley. Estimó que dado lo complejo de la protección de datos personales, éstos no deberían radicarse en un organismo gubernamental, como lo es el Ministerio de Hacienda. Aseveró que la mencionada protección, debiera radicarse en un organismo autónomo.

Concluyó su intervención enfatizando que en el proyecto de reforma constitucional se configura un estatuto de órganos autónomos, para que organismos como el Consejo para la Transparencia; el Servel; el Registro Civil y otros, estén dentro de una matriz constitucional que señale cuáles son sus ámbitos, niveles de autonomía e independencia y sus coordinaciones con los órganos públicos.

A continuación, **el Honorable Senador señor Espina** felicitó al señor Subsecretario del Ministerio de Hacienda por su exposición y solicitó que esta iniciativa tuviera prioridad para la Comisión.

Expresó que estamos ante dos derechos en pugna que se encuentran desbalanceados actualmente. Agregó que, por un lado encontramos el derecho a la información, a la transparencia, y por el otro, el derecho legítimo de los ciudadanos a la protección de sus datos personales.

Discrepó con el Honorable Senador señor Larraín, puesto que no resulta conveniente que bajo una misma institución existan dos cabezas que estarán inevitablemente en pugna.

Al respecto, puntualizó que la institucionalidad que vela por la transparencia resguarda intereses que en algunas ocasiones son contrarios a los de la protección de datos personales.

Aseguró que un punto que debe ser resuelto consiste en determinar qué sucede en caso de conflicto de competencia. Señaló que el daño es grande cuando un dato es privado y se hace público. Advirtió que los mecanismos de resolución de conflicto en ocasiones se dilatan eternamente.

Expresó que la autonomía que se le otorgue a la institucionalidad de protección de datos personales debe estar debidamente garantizada.

En relación al procedimiento, advirtió que en el proyecto de ley no se fijan plazos para dictar la resolución que le corresponda a la nueva institucionalidad.

Se mostró contrario a incorporar la posibilidad de que la Corte de Apelaciones respectiva pueda abrir un término de prueba en el procedimiento de reclamación judicial. Constató que ello implicaría extender el procedimiento. Por lo mismo, solicitó que se acote este aspecto del proyecto.

En seguida, consultó si existen medidas cautelares en caso de que se difunda un dato personal que afecte a una persona. Sobre lo mismo, inquirió si se puede obligar a una entidad a que deje de publicar un dato que es erróneo o falso.

Concluyó manifestando que en relación a las sanciones, éstas deben ser duras, ya que el uso de información que se utiliza para fines diversos constituye un abuso en contra del derecho a la privacidad de las personas.

El Presidente de la Comisión, Honorable Senador señor Harboe, también agradeció la exposición del Subsecretario del Ministerio de Hacienda, señor Micco.

Señaló que la presente iniciativa avanza decididamente a elevar los estándares de la institucionalidad en materia de datos personales. Estimó que no es casualidad que se haga un reconocimiento explícito a que la propiedad de los datos pertenece a las personas y no a las empresas que actualmente los administran.

Expresó que la consagración del principio de finalidad constituye una herramienta fundamental. Sostuvo que a pesar de que el mencionado principio se encuentra consagrado por la legislación vigente, la falta de institucionalidad, de acción, de protección real y la evolución tecnológica hace imposible pesquisar la administración y almacenamiento ilícito de datos personales.

Consignó que el proyecto de ley viene a regular de mejor manera el principio antes señalado y a generar un efecto disuasivo, a través de la creación de una autoridad y un régimen de sanciones.

Destacó que hoy tenemos verdaderos tráficos de datos. Aseveró que estamos en presencia de un negocio muy bien estructurado que puede perjudicar a muchas personas.

Agregó que si logramos aprobar el proyecto de ley en discusión, Chile debiera ser considerado un país seguro en materia de protección de datos a nivel internacional. Advirtió que desde el punto de vista penal hay instituciones internacionales que no entregan los datos ni al Gobierno, ni al Ministerio Público ni a las Policías, porque consideran que nuestros estándares de protección de datos personales no son adecuados. Precisó que lo descrito también ocurre en materia económica.

Connotó que es relevante que se contemple normativa respecto la transferencia transfronteriza de datos. Subrayó que la presente iniciativa también generará certeza en la industria relacionada con las materias consideradas en ella.

Asimismo, sostuvo que el proyecto de ley debiera mejorar la calidad de la información. En este sentido, remarcó que es cuestionable lo que realizan algunas empresas privadas.

Advirtió que la iniciativa en estudio no contempla nada en materia de datos comerciales, ello sí lo hace la Moción presentada por los Honorables Senadores señores Harboe, Araya, De Urresti, Espina y Larraín.

En cuanto a la institucionalidad, relató que es un tema que se discute hace varios años. Reseñó que le correspondió participar en un debate el año 2005 en el Consejo para la Transparencia, respecto si este organismo debía hacerse cargo de la protección de datos.

Se declaró ferviente partidario de la estructura consecuencial. Advirtió que en Chile cada vez que se detecta un problema se crean instituciones. Éstas lo que hacen es establecer un marco de acción y el objetivo que se busca no se cumple.

Reconoció que se debe dar una discusión profunda respecto a cuál es el objetivo, y a partir de ahí, crear una institución, siempre que sea necesario hacerlo. Coincidió con el Honorable Senador señor Espina en cuanto a que la autonomía no es garantía de calidad.

Sostuvo que dada la importancia que significa para la vida cotidiana la exhibición de un dato personal y particularmente de

uno sensible, es importante un régimen de sanciones a aquellos funcionarios que tengan acceso a la información y que la filtren.

Al tenor de lo anterior, recordó que un expositor alguna vez dijo: “Cuando se vulnera un dato personal sucede lo mismo que cuando un hijo se enoja con su madre, sale a la calle y con un cuchillo rompe la almohada y reparte las plumas, y después se arrepiente.”. Esa información es muy difícil de recuperar y reparar el daño causado.

Enfatizó que cuando un dato personal sensible es publicado no hay vuelta atrás. Por lo tanto, manifestó que el régimen de garantías debe quedar muy bien estructurado.

Concluyó señalando que es fundamental la aprobación de la reforma constitucional que consagra el derecho de protección de los datos personales. Ella será un paragua que permitirá que el presente proyecto de ley fluya y sea aplicable por todos los órganos de la Administración.

En una sesión posterior, e**l Presidente accidental de la Comisión, el Honorable Senador señor De Urresti,** ofreció la palabra a **la Subsecretaria de Evaluación Social, señora Heidi Berner**.

La señora Subsecretaria comenzó su exposición señalando que su presentación abarcará cuatro puntos principales, a saber:

1.- Contexto de la protección de datos;

2.- Principales aspectos del proyecto de ley;

3.- Contribuciones del proyecto de ley a la función pública, y

4.- Conclusiones.

Respecto al contexto de la protección de datos, manifestó que es indudable la necesidad de contar con una legislación de protección y tratamiento de datos personales que responda a los desafíos actuales y que incorpore dentro de sus estándares las recomendaciones internacionales y las mejores prácticas implementadas en la materia.

Agregó que los cambios experimentados por la sociedad global que incluyen avances sustantivos en las tecnologías de la información, y en los cuales la economía digital y los flujos de información son cada vez más relevantes en los procesos de producción e intercambio, en que al sector público se le exige también mayores grados de eficiencia y

eficacia, se han traducido en que la actual legislación requiera de perfeccionamientos.

Expresó que la iniciativa en estudio se hace cargo de una serie de aspectos que resultan relevantes, incorpora recomendaciones de la OCDE y logra un adecuado equilibrio entre la protección de datos, la seguridad de la información, la responsabilidad en el acceso y tratamiento de datos y la fiscalización del cumplimiento de las normas.

A continuación, destacó los objetivos que persigue esta iniciativa:

a.- La protección y derechos de los titulares de datos personales.

b.- El tratamiento de datos personales, la seguridad de la información, y la institucionalidad que permitan reforzar los derechos de los titulares de datos personales.

c.- Una legislación moderna y flexible en consonancia con los compromisos internacionales, especialmente con el ingreso a la OCDE.

d.- Definición de estándares regulatorios y condiciones para legitimar el tratamiento de datos personales por parte de los órganos públicos, compatibilizando el cumplimiento de la función pública y los derechos de los ciudadanos.

e.- Una autoridad de control de carácter técnico y una institucionalidad pública que asuma los desafíos regulatorios y de fiscalización en materia de protección de las personas y el tratamiento de los datos personales.

Añadió que en la última década se han producido grandes cambios tecnológicos en el tratamiento de datos personales.

Indicó que en el sector público, los servicios que se entregan requieren interacción digital entre las instituciones públicas y privadas, además de la necesidad de ir ampliando los servicios *on line* a los ciudadanos. Apuntó que los diversos trámites deben permitir el resguardo adecuado de los datos personales.

Ejemplificó con el Registro Social de Hogares, que reemplazó a la Ficha de Protección Social, y que hoy, además de tratar datos y conectarlos con distintas instituciones públicas, posee plataformas de trámites *on line* para que sean utilizadas por los ciudadanos.

Hizo presente que un desafío para la institucionalidad actual consiste en que nuestro país cuente con un organismo que supervise el correcto tratamiento y protección de los datos personales.

Señaló que el objeto de esta iniciativa es regular el tratamiento de datos personales que realizan las personas naturales o jurídicas, públicas o privadas, con el propósito de asegurar el respeto y protección de los derechos y libertades de quienes son titulares de estos datos. Precisó que se establece el carácter supletorio de esta normativa, en aquellos tratamientos de datos regulados en leyes especiales.

Añadió que se excluyen de este régimen el tratamiento de datos personales que se realicen en el ejercicio de las libertades de opinión y de información, y el que efectúen las personas naturales en relación con sus actividades personales.

Sostuvo que la iniciativa recoge los siguientes principios rectores que han sido reconocidos en las directrices de la OCDE:

1.- Principio de licitud de tratamiento
2.- Principio de finalidad
3.- Principio de proporcionalidad
4.- Principio de calidad
5.- Principio de responsabilidad
6.- Principio de seguridad
7.- Principio de información

A continuación, destacó que en ella se reconocen al titular de datos personales los derechos de acceso, rectificación, cancelación, oposición y portabilidad (derechos ARCOP)

Consignó que se refuerza la regulación del denominado “derecho al olvido” en relación a los datos relativos a infracciones penales, civiles y administrativas.

Respecto a la legitimidad del tratamiento de los datos, destacó el consentimiento inequívoco, que se refiere a que éste debe ser libre e informado y debe ser otorgado en forma previa al tratamiento y específico en cuanto a su finalidad.

Remarcó que se consagran excepciones al consentimiento, a saber:

- El tratamiento se refiere a datos que han sido recolectados de una fuente de acceso público.

- Cuando se trate de datos relativos a obligaciones de carácter económico, financiero, bancario o comercial y su tratamiento se realice en conformidad a la ley.

- Cuando el tratamiento sea necesario para la ejecución o complimiento de una obligación legal o de un contrato en que es parte el titular.

Manifestó que otro aspecto relevante de esta iniciativa consiste en las obligaciones y deberes de los responsables de los datos. Ellas son las siguientes:

- Acreditar, en caso que sea requerido, la licitud del tratamiento.

- Asegurar el cumplimiento del principio de finalidad.

- Comunicar información veraz, completa y actualizada de los datos personales.

- Reserva y confidencialidad.

- Información y transparencia.

- Adoptar medidas de seguridad.

- Reportar las vulneraciones a las medidas de seguridad.

Seguidamente, resaltó que se establecen estándares diferenciados de cumplimiento de los deberes de información y de seguridad, considerando si el responsable del dato es una persona natural o jurídica, el tamaño de la empresa y el volumen y finalidad de los datos que se tratan.

En cuanto a la cesión o transferencia de las bases de datos, detalló que la iniciativa regula los requisitos, modalidades de ejecución, formalidades y efectos jurídicos de la cesión de datos. Precisó que se establecen los efectos jurídicos y el régimen de responsabilidad del tratamiento de datos que efectúa un tercero en representación del responsable.

En relación al *Big Data* o tratamiento automatizado de datos, estimó que el presente proyecto de ley protege la facultad de control del titular sobre su propia información y también reconoce la licitud

del acceso y uso de información por parte de terceros y particularmente, de las empresas.

Respecto al tratamiento de datos personales sensibles destacó que se eleva el estándar para el tratamiento de éstos en relación a los demás datos personales, estableciendo que solo puede realizarse cuando el titular a quien conciernen los datos sensibles preste su consentimiento libre e informado en forma expresa.

Asimismo, continuó, se reconoce la necesidad de avanzar en la protección de algunos datos sensibles más específicos en los que se han generado significativos avances en el desarrollo científico y tecnológico, se introducen normas especiales para el tratamiento de los datos personales relativos a la salud, los datos biométricos y los datos relativos al perfil biológico humano.

Agregó que se introduce una regla especial para el tratamiento de datos personales con fines históricos, estadísticos, científicos y para estudios o investigaciones que atiendan al interés público.

Connotó que se establecen normas para el tratamiento de los datos personales de geolocalización o de movilidad del titular, sobre la base del consentimiento como fuente de legitimidad del tratamiento.

Subrayó que se introduce una regulación especial para el tratamiento de los datos personales de los niños, niñas y adolescentes, estableciendo que este solo puede realizarse atendiendo al interés superior de ellos y al respeto de su autonomía progresiva.

Asimismo, hizo presente que no se modifica la actual regulación para el tratamiento de datos referentes a obligaciones económicas.

Alabó la creación de una institución especializada, unipersonal, de carácter técnico, denominada Agencia de Protección de Datos Personales.

Luego, añadió que se consagra un modelo de coordinación regulatoria con el objeto de evitar o precaver conflictos de normas y asegurar la coordinación, cooperación y colaboración entre la Agencia de Protección de Datos Personales y el Consejo para la Transparencia.

En cuanto a las contribuciones del proyecto de ley a la función pública, manifestó que en el Título IV de la iniciativa viene a reforzar y potenciar el desarrollo de las funciones públicas de tratamiento de

datos personales, en un marco de mayores exigencias y responsabilidad respecto de los derechos que se reconocen a los titulares de los datos.

En ese sentido, destacó los siguientes elementos:

- Se regula la legitimidad del tratamiento de datos personales que efectúan los órganos públicos. Es lícito el tratamiento de los datos personales cuando se realiza para el cumplimiento de sus funciones legales, dentro del ámbito de sus competencias y de conformidad a las normas legales correspondientes.

- Se promueve la interconectividad y la eficiencia en la gestión pública, regulándose con precisión la facultad de los órganos públicos para comunicar o ceder datos personales específicos o bases de datos a otros órganos públicos, siempre que la comunicación o cesión de los datos resulte necesaria para el cumplimiento de funciones legales y ambos órganos actúen dentro del ámbito de sus competencias.

Consideró como fundamental este último aspecto. Precisó que el modelo debe propender a que cada día se solicite menos información al ciudadano y se ocupe de mejor forma la que ya se tiene.

Agregó que esta iniciativa consagra y regula los principios que rigen el tratamiento de los datos personales por parte de los órganos del Estado, los derechos que se reconocen a los titulares de datos, la forma de ejercer sus derechos y se define un procedimiento de reclamación administrativa y de tutela judicial efectiva para el ejercicio y protección de estos derechos.

Asimismo, se eleva el estándar de cumplimiento y se define con precisión la responsabilidad de los órganos públicos, se establece que el jefe superior del servicio debe velar para que la institución pública realice el tratamiento de los datos personales con arreglo a los principios y obligaciones fijadas en la ley.

Se regula un régimen de excepción para el tratamiento de datos que acometen los órganos públicos (datos protegidos por normas de secreto o confidencialidad; tratamiento de datos vinculados a la investigación de infracciones penales, civiles y administrativas; seguridad de la nación, el orden público o la seguridad pública; estado de catástrofe o estado de emergencia).

Seguidamente, afirmó que el Ministerio del Desarrollo Social cumple con los más altos estándares en relación a la seguridad de la información y al tratamiento de los datos.

Consignó que dentro de las diversas funciones que tiene el Ministerio antes mencionado, existen tres que se vinculan directamente con el proyecto de ley en estudio. Ellos son:

1.- El artículo 5° de la ley N° 20.379 que crea el Sistema Intersectorial de Protección Social e Institucionaliza el Subsistema de Protección Integral a la Infancia “Chile Crece Contigo” que indica: “El Sistema contará con un instrumento que permita la caracterización socioeconómica de la población nacional, según lo establezca un reglamento expedido a través del Ministerio de Planificación, suscrito, además, por el Ministro de Hacienda. Dicho instrumento deberá considerar, entre otros, factores de caracterización territorial”; y

2. El artículo 3°, letra f) de la ley N° 20.530, que Crea el Ministerio de Desarrollo Social, en que se señala que corresponderá al Ministerio “Definir los instrumentos de focalización de los programas sociales, sin perjuicio de las facultades de otros ministerios a estos efectos”.

Remarcó que lo anterior corresponde a lo que se conocía como la ficha de protección social, que nunca tuvo un reglamento acorde a esta normativa.

Hizo presente que actualmente cuentan con un reglamento que regula el Sistema de Apoyo a la Selección de Usuarios de Prestaciones Sociales, conocido como el Registro Social de Hogares que vino a reemplazar la ficha de protección social.

Añadió que lo anterior permite que el Ministerio de Desarrollo Social reciba información de parte de otras entidades públicas. Connotó que este procedimiento permite al Ministerio contar con un sistema moderno, simple, transparente y eficiente a la hora de generar un instrumento de caracterización socioeconómica.

Sostuvo que esta iniciativa viene a reforzar los estándares sobre los cuales se puede hacer el tratamiento de datos e interconectar distintas bases, lo que permitirá modernizar la forma en que se desarrolla el Estado con los ciudadanos, evitando volver a solicitar información que ya se encuentra en el sistema.

3.- El artículo 6° de la ley N° 19.949, en que se señala “Créase un registro de información social, diseñado, implementado y administrado por MIDEPLAN, cuya finalidad será proveer de la información necesaria para la asignación y racionalización de las prestaciones sociales que otorga el Estado; el estudio y diseño de políticas, planes, programas y prestaciones sociales, como asimismo, de planes de desarrollo local, y de los análisis estadísticos que la administración de las prestaciones sociales requieran”.

Concluyó señalando que la iniciativa otorga un marco moderno y apropiado a los desafíos actuales que enfrenta el país en materia de protección de datos personales, de seguridad de la información, tratamiento y cesión de datos y crea una institucionalidad responsable de la fiscalización del cumplimiento de la normativa.

Precisó que ella incluye un título especial de tratamiento de datos personales por organismos públicos que potencia los derechos de los titulares de los datos y la seguridad de la información y su tratamiento, además de la interoperabilidad al interior del sector público.

Destacó que el tratamiento de datos personales por organismos públicos, constituye un marco adecuado y moderno para el desarrollo de manera eficiente de las funciones mandatadas por ley, al reconocerles sus atribuciones para acceder y tratar datos, promover la interoperabilidad y, al mismo tiempo, establecerle mayores estándares para el tratamiento y la seguridad de los datos.

Concluida esta intervención, **el Presidente accidental de la Comisión, Honorable Senador señor De Urresti**, ofreció la palabra al **Presidente del Consejo para la Transparencia, señor José Luis Santa María,** quien comenzó su intervención manifestando que la presente iniciativa constituye un gran avance normativo en materia de protección de datos personales, ya que eleva sustantivamente la protección de los derechos de las personas, fijando claros deberes para los responsables del tratamiento de datos personales.

Precisó que los estándares internacionales exigen como mínimo: a) Reconocer los principios de protección de datos y los derechos ARCO; b) Fijar un régimen de infracciones y sanciones que asegure el cumplimiento de la ley y, c) Crear una autoridad de control que regule, fiscalice y sancione debidamente a quien incumple la ley.

Agregó que es posible mejorar esta iniciativa en diversos aspectos técnicos. Sugirió que en materia de fuentes de acceso público se opte por una regulación taxativa, que brinde certeza tanto a los regulados como a los órganos públicos que apliquen la ley. Asimismo, reconoció, que faltan reglas de extraterritorialidad. Sostuvo que se debe tener cuidado con las excepciones que se plantean, como en el caso de investigaciones o causas penales, civiles o administrativas, puesto que la información de las personas podrían quedar sin protección.

Añadió que para el Consejo es de especial preocupación la asimetría de protección de derechos entre el sector público y el privado, tal como lo regula el proyecto del Ejecutivo.

Consignó que respecto del sector privado, la Agencia de Protección de datos conocerá del procedimiento de tutela de derechos de los titulares de datos, pero en el sector público, las personas afectadas deberán reclamar la ilegalidad ante una Corte de Apelaciones, necesitando el patrocinio de un abogado para poder alegar sus derechos, con la consiguiente carga económica que ello conlleva.

Sostuvo que la autoridad de control debe alcanzar estándares internacionales de independencia para cumplir adecuadamente su rol. Precisó que el estándar europeo exige que la dirección de una institución de esta naturaleza, no debe quedar sometida a instrucciones o influencias externas, directas o indirectas.

Finalizó su intervención puntualizando que el cambio de paradigma y el impacto regulatorio que se busca con esta legislación, aconseja que se alcancen fórmulas óptimas de autorregulación y vigencia escalonada en el tiempo. Sugirió una entrada en vigencia de la ley que permita primero instalar la Autoridad de Control, capacitar a los organismos públicos y, luego, fomentar el uso de modelos de prevención que permitan maximizar el cumplimiento de la regulación, todo antes de la aplicación de sanciones.

A continuación, **el Presidente accidental de la Comisión, Honorable Senador, señor De Urresti**, ofreció la palabra a **la Directora Jurídica del Consejo para la Transparencia, señora Andrea Ruiz,** quien comenzó su intervención resaltando el valor de las iniciativas que se refunden en este proyecto de ley.

Manifestó que el derecho de protección de datos debe estar bien regulado, porque actualmente los titulares del mismo ven resguardado su derecho por la legislación vigente, pero lamentablemente desconocen su existencia y no saben cómo ejercer los derechos que se les reconocen. Recalcó que quien no cuenta con esta información debe incurrir en importantes costos administrativos, económicos y judiciales.

Señaló que la jurisprudencia de nuestras Cortes termina siendo una anécdota más que una realidad. Explicó que sólo en algunos casos y a instancia de organizaciones no gubernamentales o instituciones públicas, se ha logrado proteger determinados derechos. Reiteró que la mayoría de los ciudadanos ignora los mecanismos más eficaces para protegerlos.

Afirmó que aquellos que realizan un tratamiento de datos, los utilizan de manera indiscriminada. Advirtió que se sienten dueños de los datos personales y no comprenden que éstos tienen un titular.

Sostuvo que hay estándares internacionales ya fijados y que están consignados en ambas iniciativas. Ambas reconocen los principios y los derechos ARCO.

Hizo presente que el proyecto de ley del Ejecutivo crea una autoridad de control, porque es esencial que exista un ente garante de los derechos de los ciudadanos, que fiscalice y sanciones cuando corresponda.

Consideró que ambos proyectos pueden ser mejorados en diversos aspectos técnicos. Señaló que el Consejo para la Transparencia, desde su creación, ha aplicado la Ley sobre Protección de la Vida Privada, además de la Ley sobre Acceso a la Información Pública. Reconoció que lo han hecho con aciertos y desaciertos, porque no es fácil aplicar una norma tan antigua a las nuevas realidades.

Luego, aseveró que el Consejo puede aportar algunas ideas para mejorar esta iniciativa.

En cuanto a la regulación de las fuentes de acceso público, consignó que se ha producido una larga discusión respecto a qué se entiende por tal. Lamentó que ella se radique en el caso particular y no se analice la globalidad de la problemática. Sostuvo que lo ideal es que exista una regulación taxativa de dichas fuentes, puesto que entregárselos a la Autoridad de Control significará judicializar la discusión y donde las Cortes resuelven con criterios disímiles.

Asimismo, aseveró que las normas de extraterritorialidad en la legislación comparada se encuentran muy reguladas. Se preguntó qué sucederá cuando los datos sean tratados por una entidad extranjera. Expresó que ello corresponde a una excepción que debe estar regulada en este proyecto de ley.

Añadió que lo relevante no es dónde está el ente que trata el dato, sino que dónde está ubicado el titular del derecho. Lo anterior debiese garantizar la aplicación del régimen jurídico completo.

Estimó que hay que ser cuidadosos al establecer las excepciones a la aplicación de la ley. Aseveró que es mejor primero excepcionar tipos de tratamientos específicos.

Asimismo, hizo presente que resulta elemental que esté recogida la autodeterminación informativa.

En relación a la definición de los datos sensibles, consideró importante complementarla, siempre regulando aquellos casos que

están en la discusión, como la afiliación sindical. Destacó que esta última solo está recogida en la moción.

Recalcó que para el Consejo es de especial preocupación la asimetría de protección de derechos que se da entre el mundo público y privado. Apuntó que corresponde a un tema esencial cuando vemos la forma en que se garantiza un derecho fundamental como la protección de datos. Subrayó que se debe establecer caminos homogéneos a las personas para evitar que tengan distintos costos para ejercer los derechos y para que no se vean enfrentadas a decisiones contradictorias.

Connotó que la Agencia de Protección de Datos que se crea solo puede conocer de los procedimientos de reclamo del sector privado y no del público. Añadió que cuando el ciudadano que se ve enfrentado a un órgano de la Administración del Estado, debe recurrir de ilegalidad ante la Corte de Apelaciones respectiva, situación que tiene un costo que no todos pueden asumir.

En cuanto a la naturaleza de la autoridad de control, señaló que el Consejo para la Transparencia estima que ella debe ser acorde a los estándares internacionales, y éstos exigen que ella tenga independencia para el cumplimiento de sus funciones.

Agregó que el estándar europeo exige que la dirección de este tipo de instituciones no puede ser susceptible de instrucciones o influencias internas o externas, directas o indirectas. Es decir, la autoridad debe tener la suficiente capacidad para resolver con independencia los problemas que se le presentan.

Precisó que la mencionada independencia ayudaría a superar la asimetría descrita entre el sector público y privado.

Añadió que el cambio de paradigma que representa la regulación en estudio, requiere necesariamente que se alcancen fórmulas óptimas de autorregulación. Ello significa que todos los mecanismos de autorregulación deben ser capaces de incentivar al sujeto obligado a cumplir espontáneamente con la legislación. Reafirmó que el esfuerzo que éste haga debe compensarse. Es decir, debemos ser capaces de graduar las sanciones en función de ese buen o mejor comportamiento respecto de las empresas.

Por último, se refirió a la vigencia escalonada de la ley en el tiempo, indicando que el proyecto de ley debiese contemplarla, con la finalidad de que las empresas se adecuen a su cumplimiento, para que alcancen los estándares de regulación necesarios, además, de otorgarle tiempo a la autoridad de control para constituirse.

Seguidamente, **el Presidente accidental de la Comisión, Honorable Senador señor De Urresti**, ofreció el uso de la palabra **al Fiscal de la Asociación de Bancos e Instituciones Financieras, señor Juan Esteban Laval**, quien comenzó su intervención expresando que la Banca valora la presentación de ambos proyectos de ley, ya que éstos permiten adecuar la normativa vigente a los estándares legales internacionales.

Declaró que recientemente, la Superintendencia de Bancos e Instituciones Financieras publicó y presentó ante el Congreso Nacional, el tercer informe anual acerca del impacto de la ley que regula la tasa máxima convencional.

Agregó que el informe destaca que la ley ha generado una baja significativa en la mencionada tasa, pero al mismo tiempo, el número de personas potencialmente excluidas del acceso al crédito formal, a partir del cambio legal, se ubicaría entre 151 y 227 mil clientes, siendo los más afectados los clientes de más bajos ingresos (tramo 0 a 50 UF)

Opinó que lo resultados anteriores podrían mitigarse si se contara con más y mejor información. Sostuvo que las restricciones al uso de la información podrían traducirse en mayores provisiones y requerimientos de capital. En consecuencia, afirmó, la nueva regulación debe promover que los oferentes cuenten con información que permita reflejar la verdadera situación financiera de las personas

En relación a los beneficios de una mejor información, manifestó que ello acarreará un mayor acceso al crédito, ya que los oferentes de crédito cuentan con más y mejor información del deudor al momento del otorgamiento de un crédito.

Añadió que la comunicación y tratamiento de información positiva de oferentes relevantes de crédito y de otras fuentes permite una mejor gestión de riesgos por parte de las instituciones financieras y facilita la inclusión financiera; constituye una herramienta valiosa para la supervisión financiera; reduce el costo del crédito para los pagadores con historial positivo; y fomenta competencia en el mercado de crédito, facilitando la movilidad entre oferentes.

A continuación, sostuvo que los criterios ordenadores de la regulación en materia de protección de datos son los siguientes:

1) Equilibrio entre la libre circulación de la información con la protección de los derechos de los titulares;

2) Promover y velar por la calidad de los datos;

3) Contar con una institucionalidad robusta que regule y supervise el correcto uso de los datos; y

4) Velar por una adecuada coordinación regulatoria.

En relación al equilibrio entre la libre circulación de la información con la protección de los derechos de los titulares, precisó que es importante que los oferentes de crédito puedan contar con más información, pero resguardando los derechos de los titulares, a través de los principios de finalidad, calidad de los datos y proporcionalidad

Agregó que en este sentido, se debe distinguir entre las diferentes operaciones de tratamiento de datos y su finalidad. Destacó que si bien inicialmente la información se encuentra asociada a las personas, una vez que el modelo está construido, se produce la cancelación de la relación entre la persona y el dato. Por lo tanto, aseguró que la regulación debe ser capaz de permitir el desarrollo de modelos que son coherentes las mejores prácticas internacionales.

Aseveró que restringir la cantidad de información afecta especialmente a los hogares de menos recursos, porque dificulta su inclusión financiera.

En cuanto al segundo principio mencionado, indicó que la regulación debe promover y velar por la calidad, oportunidad y suficiencia de la información. En ese aspecto destacó que la caducidad de los datos debe ser consecuencia de que éstos han perdido su aptitud para proveer información de calidad y no determinarse en función del transcurso de un plazo determinado. Connotó que es relevante que se pueda contar con información porque ella permite desarrollar modelos y éstos facilitan una mayor inclusión financiera y un mayor acceso al crédito a tasas más convenientes.

Consignó que la prescripción de la acción para ejercer un determinado derecho no debe ser causal de caducidad del dato.

En cuanto a la institucionalidad que regule y supervise el correcto uso de los datos, expresó que ella debe contar con un nivel de robustez equivalente a las potestades que se le confieren.

Sostuvo que si se revisa el proyecto del Ejecutivo, se advierte que se le confiere a la Agencia de Protección un cúmulo de facultades, tales como regular, interpretar, fiscalizar, sancionar, etc. que pareciere que constituyen atributos propios de una Superintendencia.

Manifestó que lo anterior, exige que la institucionalidad de la Agencia sea robusta. Para ello estimó como imprescindible que se estudie la posibilidad de que ella esté a cargo de un órgano colegiado; que la designación de sus miembros se haga con un mecanismo equivalente al del Consejo del Banco Central.

Agregó que no le parece conveniente que en la determinación de responsabilidades se distinga entre público y privado, ya que un mismo hecho podría resolverse de distintas maneras dependiendo de quién sea el que conozca del asunto. Aseveró que el modelo propuesto por el Ejecutivo solo se conoce en países muy alejados de los parámetros de la OCDE.

En relación a la coordinación regulatoria, ratificó que el proyecto del Ejecutivo solo contempla la coordinación regulatoria entre la Agencia de Protección de Datos Personales y el Consejo para la Transparencia. Sin embargo, sostuvo que las decisiones de la Agencia no solo impactarán en materias de acceso a la información pública.

Remarcó que el recurso de ilegalidad ante la Corte de Apelaciones no es suficiente. Opinó que la nueva institucionalidad que se crea con la Agencia de Protección de Datos Personales, exige que se establezcan mecanismos de contrapeso al ejercicio de sus facultades (equivalente al modelo *check and balances* de la Comisión para el Mercado Financiero – informe previo Banco Central)

Añadió que sin perjuicio que la ley que crea la Comisión para el Mercado Financiero incorporó a nuestra legislación el principio de coordinación regulatoria entre los órganos de la Administración del Estado, dicho principio se debe fortalecer a través del carácter vinculante del informe del órgano consultado.

Concluyó su intervención agradeciendo la invitación formulada por la Comisión y manifestó su disposición a colaborar en la tramitación de las iniciativas en estudio.

A continuación, **el Presidente accidental de la Comisión, Honorable Senador señor De Urresti,** ofreció la palabra **al Presidente de la Cámara Nacional de Comercio, señor Ricardo Mewes**, quien agradeció la invitación de la Comisión.

Manifestó que la protección de los datos de las personas, así como el libre flujo de información, son temas de gran preocupación para la Cámara, debido a que la correcta identificación de quienes requieren productos o servicios de las áreas que representan, constituye un atributo esencial de las relaciones comerciales.

Agregó que dicha información permite avanzar en la generación de propuestas que están más acordes con las necesidades de esas personas y garantiza, de mejor manera, la satisfacción de éstos en las relaciones de consumo.

Hizo presente que la información permite conocer los gustos y preferencias de esas personas y ofrecer a éstos productos y servicios que responden de mejor manera a los requerimientos que cada uno de ellos formula.

En ese orden de ideas, expresó que estamos experimentado el avance hacia una sociedad en que el comportamiento de los consumidores, está dejando de ser parte de una fórmula que alimenta un programa computacional y se está transformando en un elemento clave, en la diferenciación que hoy se exige, por parte de los consumidores en las nuevas relaciones de consumo.

Consignó que el acceso y gestión de los datos de las personas permiten al comercio, los servicios, el turismo otorgar a éstos un trato especial e individual el cual hoy se desarrolla mediante las nuevas herramientas tecnológicas sobre las cuales se prevé se desarrollen estas actividades durante el futuro cercano y de las cuales, hoy el *e-commerce*, constituye la mejor de sus manifestaciones.

Asimismo, connotó que lo anterior se traduce en que hoy enfrentamos un escenario muy competitivo, en el cual la oferta de productos y servicios no se mide solo por el resultado de corto plazo, sino que la oportunidad, la gestión de consultas, la atención de reclamos y la consideración a la individualidad, se convierten en la clave del éxito de las empresas y marcan la diferencia entre las experiencias exitosas y aquellas que quedan en el camino.

Aseveró que el acceso a la información y el desarrollo de las nuevas tecnologías conllevan una gran responsabilidad. Añadió que la individualidad de los consumidores demanda respeto a sus derechos, especialmente a su privacidad.

Seguidamente, expresó que la Cámara Nacional de Comercio concurre ante la Comisión con la convicción que la discusión que hoy se inicia, debe tener como orientación la existencia de un sano equilibrio entre la intimidad y el acceso a la información. Este acceso no encuentra sentido y carece de valor, sino se enfoca en las personas.

Indicó que un desequilibrio hacia la circulación de información terminará invadiendo los espacios personales de los

consumidores los que abandonarán a aquellas empresas que no comprendan esta situación.

Declaró que un desequilibrio hacia la intimidad terminará impidiendo el debido desarrollo de mejores productos y servicios y ahogará la iniciativa del emprendedor, el que al no poder acceder a las preferencias y datos de sus potenciales clientes, verá frustrados los esfuerzos por darse a conocer. En este escenario se propende a la concentración al constituir la información una infranqueable barrera de entrada al mercado.

Advirtió que a la Cámara que representa le preocupa de especial manera la situación de la pequeña empresa, la que puede ver frustrados sus esfuerzos por darse a conocer en el marco de una economía en que el consumidor exige un contacto directo y personalizado.

En el marco de lo ya expuesto, sostuvo que ambas iniciativas son claramente un avance importante, pero ellas pueden ser objeto de perfecciones durante su tramitación y que es importante que durante ésta, se tenga siempre en vista el equilibrio entre los derechos que están en juego.

Indicó que se referirá en esta oportunidad, solamente a aquellos aspectos que, de una primera lectura, destacan sobre otros. Ellos son: la formación del consentimiento, la cesión de datos personales, los sujetos obligados, la determinación de las multas y la Agencia de Protección de Datos Personales.

En relación a la regulación de la formación del consentimiento, manifestó que para el comercio es de la mayor relevancia contar con un procedimiento de obtención y verificación del consentimiento lo más simple y transparente posible. En consideración a lo anterior, estimó que se debe avanzar en un modelo fundado en la prueba documentaria a uno que permita la utilización de nuevas tecnologías.

Añadió que también es relevante que se permita esta manifestación mediante “un acto afirmativo que dé cuenta con claridad de la voluntad del titular”. En este punto eso sí, estimó importante dotar a este concepto de mayores precisiones con el propósito de evitar diferencias de interpretación que seguramente se producirán al minuto de aplicar la disposición.

Aseguró que los alcances relativos a quién puede tratar los datos personales y con qué propósito, son claves en las relaciones comerciales modernas.

Asimismo, consignó que es imprescindible que el titular de los datos entienda estas variables al minuto de otorgar su consentimiento, pero debemos ser cuidadosos con pretender un conocimiento detallado de estas variables en el marco, por ejemplo, de un contrato de adhesión.

Enfatizó que es importante tener presente que existe un fino equilibro que cuidar entre la cantidad de información a entregar y la generación de nuevas iniciativas comerciales. Insistió que el exceso de información causa desinformación.

Subrayó que la correcta protección de los derechos de los titulares, especialmente en lo que respecta al otorgamiento de una voluntad libre e informada, se logra no solo mediante la entrega de grandes cantidades de información sino que también a través de la obligación que recae sobre el responsable de la base de datos de demostrar que se cuenta con tal consentimiento, circunstancia que refuerza la idea de la protección y licitud del tratamiento de los datos personales y genera responsabilidades asociadas para los infractores y, a su vez, mediante el debido ejercicio de los derechos de cancelación y oposición.

Declaró que parece relevante efectuar alguna aclaración en lo que dice relación con la operación del denominado principio de proporcionalidad. Agregó que si bien conceptualmente no podemos sino compartir su inclusión, se debe cuidar que bajo la aplicación del mismo se fuerce a las empresas a efectuar una estimación temporal en torno a la utilización de los datos.

En efecto, expresó que si partimos de la base que las relaciones comerciales avanzan y se adaptan a las exigencias del mercado, no parece correcto exigir al inicio de las mismas, un cálculo temporal que en la casi totalidad de los casos estará fundado en un aspecto fortuito.

En relación a la cesión de datos personales, sostuvo que dado el desarrollo de las relaciones comerciales y la velocidad con que evolucionan los mercados, dicha cesión es una materia que requiere ser tratada, no solo bajo la óptica del consentimiento como lo efectúa el proyecto del Ejecutivo.

Destacó que en esta materia, la moción en estudio avanza de manera significativa en el punto, siguiendo la tendencia internacional en la materia, al consagrar excepciones al consentimiento, lo que evita una excesiva rigidización de la cesión de datos que a la larga, afecta el libre flujo de información.

En este sentido valoró la redacción propuesta en la moción, que señala: “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.”

En cuanto a los sujetos obligados, indicó que el proyecto del Ejecutivo mantiene el concepto actualmente vigente en orden a que el responsable de los datos puede tratar directamente los mismos o bien hacerlos a través de un tercero mandatado al efecto.

Estimó como más adecuada la propuesta de la moción que distingue entre responsable y encargado, con responsabilidades definidas para cada uno. Lo anterior permitirá precisar de mejor manera los deberes que se deben cumplir en la custodia y gestión de datos.

Seguidamente, explicó que si bien en otras legislaciones se regula la figura del intermediario del tratamiento, no parece adecuada la propuesta legislativa contemplada en la Moción, de sujetar a éstos a las mismas obligaciones que a los encargados del tratamiento.

Respecto a los criterios que propone el Ejecutivo para la determinación de las multas, se estima que el punto requiere una revisión más detallada, en consideración a que parece inadecuado incluir como factores de cálculo los siguientes:

- Tratarse de persona natural o jurídica, o si se trata de una entidad sin fines de lucro.

- Parecen excesivas las sanciones en caso de reincidencia, las que a su vez, debieran ser respecto de la misma infracción o a lo menos de igual naturaleza (no confundir leves con gravísimas).

- La implementación de modelos de prevención debiera ser considerada como una eximente de responsabilidad, toda vez que existirán por parte de la Autoridad certificaciones de los mismos y revisiones constantes.

Finalmente, en relación a la Agencia de Protección de Datos Personales, señaló que es, sin lugar a dudas, uno de los temas más relevantes del proyecto de ley ya que la eficiencia de las normas dependerá de la fortaleza de la autoridad llamada a velar y fiscalizar su cumplimiento.

Agregó que así lo ha manifestado en diversas oportunidades este Congreso Nacional, no solo en la tramitación de los

presentes proyectos de ley, sino que también ante los mensajes presentados por gobiernos anteriores.

Estimó que es necesario caminar, de manera más decidida, hacia una verdadera agencia independiente en materia de protección de datos personales. Ella debe ser neutral políticamente, con gran especialización técnica y eficacia.

Recalcó que la mencionada autonomía debe reflejarse en su ámbito funcional, humano o de personal, así como en otros complementarios como son la idoneidad de su organización y sus medios financieros.

Añadió que si bien se aprecia un esfuerzo de autonomía al establecer que la referida Agencia se encuentra afecta al Sistema de Alta Dirección Pública, explicó que aún se está muy lejos de configurarse como una agencia independiente.

Sostuvo que se debiera avanzar en la generación de una entidad con una dirección colegiada y no unipersonal como se propone por el Proyecto del Ejecutivo, debiendo dedicarse los mayores esfuerzos al establecimiento de un poderoso gobierno corporativo.

Junto a lo anterior, destacó que parece necesario evitar los cuestionamientos que se pudieren formular a una repartición que junto con fiscalizar y normar, pueda imponer sanciones frente a eventuales incumplimientos. Lo anterior debido a que la convivencia de tales facultades bajo una misma dirección representa un retroceso en materia de independencia y, en algunos casos, podría comprometer seriamente el principio del debido proceso a que tiene derecho toda persona.

Concluyó su intervención señalando que no es conveniente entregar facultades sancionatorias a dicha Agencia. Ella debería poder reclamar ante los tribunales los incumplimientos a la ley o la normativa respectiva y permitiendo que sean éstos quienes resuelvan la contienda.

A continuación, **el Presidente accidental de la Comisión, Honorable Senador señor De Urresti,** ofreció la palabra a los Honorables Senadores presentes con la finalidad de que pudieran formular preguntas a los invitados a esta sesión.

En primer lugar hizo uso de la palabra **el Honorable Senador señor Larraín** quien agradeció cada una de las exposiciones, ya que en ellas se plantearon aspectos muy centrales de la iniciativa en estudio.

Agregó que la protección de datos corresponde a un tema que a esta Comisión le interesa de manera especial. Manifestó que junto al Honorable Senador señor, Harboe son autores de una reforma constitucional que se aprobó en el Senado. Ella tiene por objeto dar a la protección de datos y a los derechos que de ella deriva, un marco constitucional. Expresó su deseo que la mencionada moción se apruebe con anterioridad a los actuales proyectos en estudio. Remarcó que estos principios deben estar resguardados en el orden constitucional.

En cuanto a las iniciativas en discusión, sostuvo que hay aspectos que son valiosos y recogen el estado del debate actual. Sin embargo, declaró que las inquietudes que surgen tienen relación con los siguientes elementos:

1.- La Agencia de Protección de Datos. Ella debe ser autónoma e independiente y con un gobierno corporativo adecuado.

Aseveró que el hecho de que sea un órgano adscrito al Ministerio de Hacienda, le produce una inquietud mayor, porque entregarle a un Ministerio tan potente, que tiene una ocupación central, le produce una sensación equívoca. Se preguntó por qué toda la información relacionada con la protección de datos tendría que estar bajo el alero de un ministerio. Lo anterior, argumentó, alimenta la necesidad de elaborar un proyecto que garantice a los chilenos que sus datos personales estarán protegidos por una organización autónoma e independiente de todo organismo público.

Remarcó que así ocurre en el derecho comparado. Indicó que probablemente en sus inicios las agencias se adscribían a un Ministerio, pero ello ya no corresponde al estándar actual.

Enfatizó que la autonomía de la Agencia constituye un capítulo central. Se preguntó si la Agencia de Protección de Datos podría estar bajo el mismo alero de aquella encargada de la transparencia. Explicó que esa medida parecía razonable. Ejemplificó con el caso de Canadá, que bajo una misma institución están las dos agencias, pero operan en Salas especializadas. Añadió que están dotadas de un órgano superior que permite buscar la unidad de criterio.

Manifestó que el acceso a la información pública tiene un límite en la intimidad de los datos personales. Se trata, explicó, de dos caras de una misma moneda. Por lo mismo, abogó porque en esta materia haya una mirada común en la Comisión.

2.- Regulación. Hizo presente que ella es deficitaria y se presta para abrir espacios a la judicialización. Estimó que este último no es el camino para enfrentar y resolver estos temas.

3.- Régimen de Excepción. Aclaró que éste es particularmente incierto. Sostuvo que queda en este marco, informaciones extraordinariamente relevantes y ese ámbito de incertidumbre que se genera, origina inquietudes y preocupaciones.

Consultó a los expositores cómo advierten el tratamiento de las pequeñas y medianas empresas. Recalcó que constata que su situación está tratada de manera insuficiente, dado que no se hace una distinción que permita recoger la distinta naturaleza de ambas entidades.

En relación a la aplicación del principio de proporcionalidad y de finalidad, recordó que el Presidente de la Cámara Nacional de Comercio planteó que la temporalidad en torno a la utilización de los datos era difícil de determinar, sobre todo al inicio. Señaló que precisamente ese es el sentido de juntar los mencionados principios, en que el uso debe estar determinado para ciertos fines, porque de lo contrario, si no hay una dimensión en el tiempo quiere decir que son de uso indefinido y serán utilizados para finalidades distintas y ello abre un margen de incertidumbre para los ciudadanos, quienes no tendrán claridad respecto a cómo serán utilizados sus datos o su información.

En esta parte del análisis, **el Presidente accidental de la Comisión, Honorable Senador señor De Urresti,** preguntó cuál es el ámbito de territorialidad y alcance de este proyecto en materia de jurisdicción.

Asimismo, se mostró contrario a que la Agencia esté radicada en el Ministerio de Hacienda, ya que éste tiene otras competencias y prioridades.

El Presidente de la Cámara Nacional de Comercio, señor Ricardo Mewes señaló que, en relación al fortalecimiento de las Pymes, hoy en día, se hace muy complejo llegar al consumidor final en un mundo tecnológico y globalizado. Añadió que dicho emprendedor verá frustrada su opción porque no podrá competir con las grandes empresas que llevan años generando antecedentes e información respecto al consumidor.

Estimó que se deben crear los espacios para que las pequeñas y medianas empresas se puedan desarrollar. Agregó que si se determina claramente lo que se entiende por finalidad, el emprendedor podrá contar con su base de datos para ofrecer sus productos. Se mostró partidario de incorporar en el presente proyecto el fortalecimiento de las pymes.

En cuanto a las competencias del órgano público que crea este proyecto, advirtió que está a favor de una Agencia autónoma.

Reconoció que ello favorecería que los tribunales se pronuncien sobre el fondo del asunto y lo hagan de un modo imparcial.

Por su parte, **la Directora Jurídica del Consejo para la Transparencia, señora Andrea Ruiz** sostuvo que la territorialidad es una materia que se trata en todos los textos que regulan los temas de protección de datos, porque se entiende que, en general, los datos no reconocen fronteras, ellos circulan libremente, por tanto, es necesario regular no solo lo que ocurre en Chile, sino que también lo que sucede con los datos de los residentes en el extranjero. Así, reseñó que existe una serie de normas en la Unión Europea que recoge la situación de los bienes y servicios prestados en un determinado país por un extranjero y, en ese caso, se aplica la territorialidad.

Connotó que el almacenamiento de datos en la nube se produce generalmente por una empresa extranjera, en ese contexto preguntó bajo qué legislación quedarán regulados los datos. Recalcó que de ahí surge la necesidad de consagrar normas que contemplen la extraterritorialidad.

Asimismo, consideró relevante que la Agencia tenga una autonomía técnica. Declaró que el hecho de tener una Agencia de Protección de Datos y un Consejo para la Transparencia podría implicar que los dos órganos terminen transformando sus egos institucionales en sus decisiones y se termine discutiendo todo en las Cortes de Apelaciones, es decir, lo que sea público o reservado en virtud de la protección de datos termine siendo resuelto por los tribunales de justicia.

Agregó que, por lo anterior, resulta relevante coordinar ambas competencias en un mismo organismo, para evitar ese tipo de asimetrías.

Luego, **el Honorable Senador señor Larraín** consignó que se debe velar por la privacidad de los datos. Igualmente, se debe garantizar un mecanismo sencillo para que las personas puedan acercarse a los organismos correspondientes para proteger sus datos personales. Constató que actualmente hay muchos antecedentes en manos de agentes públicos y privados. Consideró que debe haber un organismo accesible que proteja a los ciudadanos y que no les implique mayores gastos.

Aseveró que es partidario que la Agencia esté bajo el alero del Consejo para la Transparencia, ya que las decisiones entre ambos no deben ser contradictorias, porque si bien regulan aspectos distintos, finalmente ambos se vinculan con la protección y el acceso a la información. Reiteró que esto constituye un tema central del proyecto. Hizo un llamado al Ejecutivo para que se haga cargo de él.

Afirmó que lo que no está claro es el uso y abuso que se hace de la información privada. Ahí es donde se debe poner el acento y corresponde instaurar los mecanismos adecuados. Insistió que el Gobierno no tiene resuelto adecuadamente el problema planteado.

La Subsecretaria de Evaluación Social, señora Heidi Berner manifestó que siempre se piensa que la mejor forma en que se resguardan los datos personales, es mediante un organismo autónomo. Agregó que la discusión desde el Ejecutivo consistió en plantearse si se necesitaba un organismo autónomo o uno que técnicamente fuera independiente. Sostuvo que ella es partidaria de esto último.

Hizo presente que la mencionada independencia técnica se puede llevar a cabo cuando la normativa es suficientemente clara.

La Coordinadora de Finanzas Internacionales y Mercado de Capitales del Ministerio de Hacienda, señora Bernardita Piedrabuena justificó la existencia de la Agencia de Protección de Datos Personales en el Ministerio de Hacienda, señalando que revisaron la legislación comparada y detectaron que no existe un patrón definido. Hizo presente que en la OCDE existen muchos países en que la Agencia depende del Ejecutivo. Por lo tanto, la definición de ésta dependerá de la legalidad y la cultura del país.

Enfatizó que en el proyecto se opta por el Ministerio de Hacienda, por razones de eficacia y eficiencia reguladora, es decir, en dicha Cartera, la Agencia tendrá un poder suficiente para hacer valer el cumplimiento de la ley.

El Honorable Senador señor Larraín sostuvo que originalmente no había claridad respecto a dónde ubicar a la mencionada Agencia, pero el debate tal cual ha evolucionado avanza hacia órganos autónomos. Subrayó que si el Ejecutivo está tan seguro de la independencia técnica debiese dar el paso de dotarla del estatus jurídico que tienen muchas instituciones en Chile. Dio el ejemplo del Banco Central, indicando que siendo autónomo tiene vinculaciones con el Gobierno, a través del Ministerio de Hacienda.

El Presidente del Consejo para la Transparencia, señor José Luis Santa María, connotó que el Consejo que tiene el honor de presidir, puede hacerse cargo de la Agencia de Protección de Datos, tal como ocurre en Canadá, mediante dos Salas especializadas.

El asesor del Ministerio de Hacienda, señor Roberto Godoy, aclaró que la Agencia es un órgano descentralizado que no depende del Ministerio de Hacienda, sino que se relaciona con el Presidente

de la República a través de la mencionada Secretaría de Estado. Mencionó que el Congreso Nacional recientemente aprobó la creación de la Comisión para el Mercado Financiero, cuya naturaleza jurídica es idéntica a la que se propone para la Agencia. Recalcó que estamos ante un organismo con autonomía técnica y funcional.

Agregó que desde el punto de vista de su nombramiento, la autoridad del mencionado organismo es designado mediante el mecanismo de la Alta Dirección Pública.

Reconoció que el tema a discutir es si la Agencia debe estar conformada por una autoridad unipersonal o colegiada.

En una sesión posterior, el **Presidente de la Comisión, Honorable Senador señor Harboe**, ofreció la palabra al gerente general de la Confederación de la Producción y del Comercio, **señor Fernando Alvear**, quien agradeció a los miembros de la Comisión la invitación a exponer respecto de un proyecto de ley muy relevante.

Al iniciar su intervención, manifestó que éste es un tema muy importante, no solo para el sector privado sino que para el país en su conjunto. Expresó que la ley N° 19.628 sobre Protección de la Vida Privada, si bien fue pionera en su época, hoy requiere una revisión y ajuste, lo que ha motivado que en el último tiempo se hayan presentado un sinnúmero de proyectos en la materia, entre los que se encuentran incluso tres mensajes presidenciales.

Indicó que este perfeccionamiento es imprescindible para adecuar la legislación a los vertiginosos cambios que ha tenido no solo la economía, sino que internet. Agregó que el flujo de información otorga tanto a ciertos países como empresas un poder sin precedente, siendo las más características de este nuevo paradigma, las que aparecen en la portada de la edición, de hace tan solo un par de semanas, de la prestigiosa revista *The Economist*.

A consideración de lo antes expuesto, declaró que la CPC estima que es necesario avanzar en la protección de datos, así como en materia de privacidad en general. En este contexto señaló que consideraban especialmente relevantes, las siguientes materias:

1. Otorgar un mayor reconocimiento, así como una protección más eficiente de los derechos de los titulares de datos personales;

2. Fortalecer y hacer más expeditos los procedimientos para hacer efectivos dichos derechos, así como la incorporación de sanciones que sean realmente inhibitorias de conductas contrarias a la protección de datos personales y de la privacidad;

3. Mejorar los estándares de seguridad en el tratamiento de datos, ello con el propósito de velar por la necesaria confianza en el flujo de información;

4. Facilitar y simplificar la obtención del consentimiento, para que esto no se transforme en una traba excesivamente gravosa, tomando en consideración especialmente el avance de la tecnología.

Agregó que la regulación de la protección de los datos personales debe colaborar de manera efectiva a brindar respuesta a las siguientes interrogantes:

a) ¿qué debe entenderse por dato personal? Sostuvo que éste corresponde a un concepto en constante evolución, siendo, por ejemplo, cada vez más difusa la diferencia entre datos y metadatos. Si bien hasta hace algún tiempo atrás, los metadatos, que en definitiva son datos que describen otros datos o “datos respecto de datos”, no tenían mayor relevancia, el avance vertiginoso de las tecnologías, la separación de unos u otros, es cada vez más compleja, como se puede apreciar, por ejemplo, respecto de la geolocalización que, si bien es en sí un metadato, luego de escándalos como el de la *NSA* en Estados Unidos, y su sistema de vigilancia filtrado por Edward Snowden, han hecho necesario regularlos como un dato más de la persona.

Destacó que otra interrogante que requiere constante revisión se refiere a ¿qué datos personales son comúnmente tratados? ¿Quién es, en definitiva, el responsable del tratamiento y si los estándares de seguridad exigidos a éstos, son los adecuados para la protección de los datos?

A su vez, en una sociedad cada vez más tecnologizada cabe preguntarse también ¿Por qué y para que fines se recolectan los datos personales? Esto, en consideración a que día a día, se encuentran nuevos usos a los datos de las personas. Un ejemplo de esto es la *Big Data* que ha dado uso a información antes irrelevante, como la denominada “*dark data*”, antecedentes tales como texto e imágenes pudiendo ahora ser estructurados y ser tratados como cualquier otro tipo de dato.

Argumentó que dado lo anterior, la CPC apoya la idea de legislar, ya que como los hechos lo demuestran, es imperiosa la modernización de nuestra legislación en materia de protección y tratamiento de datos personales.

Recalcó que es de suma importancia que este avance sea responsable y reflexivo, ya que debemos evitar caer en el prejuicio de que la protección de los datos personales se logra únicamente sobre el establecimiento de trabas, directas o indirectas, al tratamiento de los mismos.

Subrayó que lo anterior es de la mayor relevancia, ya que la información hoy en día constituye un activo estratégico para la actividad, tanto privada como pública y, en definitiva, para el país en su conjunto.

Así, continuó, el legítimo interés por proteger a las personas de posibles abusos no puede terminar exponiendo al país a la pérdida de una ventaja competitiva frente a otras naciones. La ley debe establecer un equilibrio adecuado entre:

1. La protección de los datos y el libre flujo de la información, y

2. La existencia de controles y el desarrollo de la iniciativa privada;

En base a todo lo anteriormente señalado, indicó que la CPC estima que el proyecto avanza de manera correcta en el establecimiento de principios rectores para el tratamiento de datos personales, aun cuando también estima que resulta importante revisar la aplicación práctica de algunos de ellos, tomando en consideración la realidad de nuestro país. Así por ejemplo, frente al principio de proporcionalidad, cabría preguntarse ¿cuál es el tiempo necesario para cumplir con los fines del tratamiento en un programa de fidelización de clientes?

Añadió que otro elemento relevante del proyecto es el reconocimiento de los derechos ARCO, los que constituyen un paso en el sentido correcto. No obstante lo anterior, explicó que le preocupaban los costos que esta iniciativa puede generar a los responsables de bases de datos. Entre estas nuevas cargas se aprecia, por ejemplo, la obligación de otorgar acceso gratuito a los titulares de los datos, de manera trimestral. En este sentido, manifestó que dicho acceso gratuito debe estar garantizado, pero el período de tiempo para hacer ejercicio de dicho derecho, debiera ser objeto de una revisión, en base a la experiencia práctica y a un debido análisis costo-beneficio de la propuesta.

En cuanto a la formación del consentimiento, connotó que comparte la idea central, tanto de nuestra legislación actual como del proyecto, en orden a que la principal fuente de autorización del tratamiento de datos personales, sea la voluntad de su titular. En este orden de ideas, es valorable la propuesta que el proyecto presenta, en orden a

avanzar desde un modelo, en que la voluntad solo puede manifestarse de manera escrita a un modelo en que puede realizarse mediante, una declaración verbal; una declaración escrita, por medios electrónico, o mediante un acto afirmativo que dé cuenta con claridad de la voluntad del titular.

Indicó que sin perjuicio de lo anterior y solo con objeto de evitar confusiones en su aplicación, resultaría conveniente otorgar más contenido a esta última expresión, ello con el propósito de evitar posibles ambigüedades en la interpretación de la norma.

Agregó que sin lugar a dudas, la creación de la denominada Agencia de Protección de Datos Personales es uno de las propuestas más importantes del proyecto.

Sin perjuicio de lo anterior, manifestó que la suficiencia de este nuevo órgano de la administración del Estado debe ser analizada tanto desde el punto de vista orgánico, como de las facultades que se le otorgan.

Así, desde el punto de vista orgánico, es una condición esencial de una adecuada agencia independiente, que se trate de una autoridad autónoma, independiente y con patrimonio propio, con objeto que su actuar se rija únicamente por consideraciones técnicas.

Para esto, consideró que un elemento esencial debe ser la “autonomía” y sus razones de existencia, la neutralidad política, especialización técnica y eficacia.

Para ilustrar este punto, citó el siguiente texto, redactado por autores de gran reconocimiento en materia de agencias independientes, quienes señalan que:

“Sería ingenuo creer que estas circunstancias políticas no se consideran cuando la relación entre el regulador y el ejecutivo es estrecha y por eso son necesarias salvaguardias adicionales para forzar a que los procesos regulatorios arrojen resultados imparciales y técnicos. La forma más directa de evitar que el ejecutivo influencie al regulador es que la agencia sea independiente, tanto formal como presupuestariamente. La incidencia formal significa que el regulador cuenta con mandato propio y no está sujeto a control ministerial. El regulador es designado por un periodo predeterminado suficientemente prolongado y no puede ser removido sino bajo circunstancias calificadas. La independencia presupuestaria requiere que la agencia regulatoria cuente con presupuesto propio cuya generación sea independiente del ejecutivo. No obstante, la independencia no garantiza que la regulación sea competente ni transparente. La selección del regulador

debe ser fundamentalmente técnica, no política y la persona seleccionada debe dar garantías de independencia.”

Consignó que de la simple lectura del texto señalado, se pueden recoger valiosas recomendaciones para perfeccionar la institucionalidad de protección de datos personales, entre las que se encuentran las siguientes:

• Establecer un gobierno corporativo de carácter colegiado y no mantener el sistema de superintendencias unipersonales superadas por la legislación comparada.

• Que la designación de los integrantes de este gobierno corporativo sea aprobada por el Senado, sistema que ha sido propuesto por la misma OCDE, como mecanismo que maximiza la autonomía de la Agencia.

• Fijar períodos de permanencia en el cargo por tiempos superiores a los del gobierno central y con causales específicas de cesación en el cargo, todo ello con el declarado objeto que su permanencia no quede sujeta a la discrecionalidad del gobierno de turno.

• Consagrar la imposibilidad que los directores interinos puedan postularse al cargo definitivo, ya que, en la práctica, esto desincentiva la postulación de terceros calificados e independientes. Esto debido a que una persona designada sin concurso previo y que luego postula por Alta Dirección Pública (ADP) necesariamente tendrá conocimientos suficientes para ser propuesto por el sistema de ADP, haciéndolo permanecer en su cargo en desmedro de terceras personas con conocimientos técnicos y autonomía respecto de la autoridad de turno.

• Generar una norma que establezca un presupuesto mínimo en la Ley de Presupuesto, con objeto de evitar presiones indirectas por parte del gobierno de turno.

Hizo presente que no avanzar en agencias independientes, no solo facilita la influencia del Gobierno en las decisiones de dicha autoridad, sino que, a su vez, dificulta la evaluación de su desempeño en materias regulatorias.

Añadió que, por ejemplo, un ente encargado tanto de fijar tarifas como de establecer las políticas públicas de desarrollo para dicho sector regulado, tendría incentivos a fijar tarifas mayores a lo socialmente conveniente, para permitir, por ejemplo, la modernización de tal sector.

Asimismo, expresó que si el organismo regulador tiene dependencia administrativa del Ejecutivo, su responsabilidad pasa a ser política más que técnica por lo que, siguiendo con el ejemplo anterior, los criterios para la determinación de las tarifas pueden no ser motivados exclusivamente por criterios de eficiencia.

Finalmente, señaló que comparte la visión que una agencia regulatoria independiente y autónoma facilita la asignación de responsabilidades específicas y el proceso de control de gestión y medición de su desempeño.

Adicionalmente indicó que también resulta pertinente revisar en profundidad las potestades reguladoras que se otorgan a la Agencia. Esto en consideración a que se le entregan facultades propias de superintendencias, las que se encuentran superadas por las legislaciones comparadas, siendo éstas, entre otras las siguientes:

1.- Dictar normas de carácter general y obligatorias;

2.- Fiscalizar el cumplimiento de la ley;

3.- Resolver reclamos, y

4.- Ejercer la potestad sancionatoria.

Destacó que esto es de la mayor importancia, en consideración a que, si bien se trata de un conjunto de facultades ya entregadas a otros entes técnicos, como el SII y la Dirección e Inspección del Trabajo, en estos casos, con el propósito de velar por un necesario sistema de pesos y contrapesos, se crearon tribunales especializados para conocer de sus resoluciones.

Asimismo, hizo presente lo que ocurrió con la Superintendencia del Medio Ambiente, la que solo comenzó a ejercer el total de sus funciones una vez que comenzaron a funcionar los tribunales ambientales.

Por lo mismo, estimó que era necesario crear tribunales especializados, o en su defecto, regular de mejor manera la creación de un ente que tendrá la facultad de dictar normas de carácter general y sancionar en base a las mismas, haciendo ilusorio el recurso de reclamación por ilegalidad ante los tribunales de justicia.

En este orden de ideas, sostuvo que debiera avanzarse de manera más decidida en el establecimiento de normas

generales que regulen el actuar de la Agencia en el ejercicio de sus funciones. En este sentido, el ejercicio de una facultad normativa por una autoridad como la que se propone en el proyecto, debiera exigir de parte de ésta, la debida justificación económica y sustancial, la realización de estudios técnicos y regulatorios y el sometimiento a un procedimiento de consulta ciudadana. De esta manera, continuó, se obtendría un estándar de justificación muchísimo más alto en el ejercicio de la facultades fiscalizadoras y sancionatorias.

Finalmente, y en relación con la regulación de las facultades otorgadas a la Agencia, expresó que si bien comparte la necesidad de velar por la protección de los datos personales frente a la ocurrencia de un evento grave que atente contra la ley, estimó necesario definir de mejor manera cuando se está en presencia de “circunstancias debidamente justificadas” que ameriten tal decisión, debido a los graves efectos que puede ocasionar el uso indiscriminado de una medida como ésta, a los responsables de las bases de datos y sus negocios habituales.

Consignó que dicha facultad debiera proceder únicamente para evitar efectos sistémicos o que pudieren generar gravísimos daños a titulares de datos.

Concluyó su intervención señalando que éstos son los elementos más relevantes del proyecto, sin perjuicio de quedar desde ya a disposición de la Comisión para aportar en el debate de una materia tan relevante.

A continuación, **el Presidente de la Comisión, Honorable Senador señor Harboe**, ofreció la palabra al **Presidente de la Asociación Chilena de Empresas de Tecnología de Información A.G., señor Raúl Ciudad,** quien comenzó su intervención agradeciendo la invitación que le formuló la Comisión para exponer en esta importante iniciativa de ley.

Seguidamente, señaló que Chile se encuentra ante la oportunidad de contar con un marco de protección de datos personales que resguarde la privacidad y que a la vez facilite los usos beneficiosos e innovadores de los datos en un entorno de negocios y tecnológico en constante evolución, lo cual en última instancia garantizará la competitividad económica del país.

Agregó que no obstante lo anterior, esta oportunidad de mejorar nuestros estándares de protección no debe implicar una sobre regulación que impida la generación de negocios innovadores, ni que se traduzca en aumentos en las estructuras de costos, especialmente para la pequeña y mediana empresa, haciéndolas menos competitivas en

relación al resto de las empresas no solo a nivel local sino también a nivel mundial.

Sostuvo que estamos enfrentados a la cuarta Revolución Industrial, que se inició a principios del año 2013 y que consiste en instalar los datos en el centro y en el eje estratégico del desarrollo del país. Recalcó que estas tecnologías provocan que toda la gestión, tanto de negocios como de las personas, dependerá de cómo se manejen, cómo se obtengan, cómo se transmitan y cómo se almacenen los datos.

Hizo presente que se hace indispensable la dictación de una ley que regule las nuevas tecnologías, tales como la movilidad; el *Big Data*; las redes sociales y la formulación de plataformas.

Manifestó que existe una revolución tecnológica invisible. Añadió que en cualquier ámbito aparece el mudo digital, y éste se manifiesta en la enorme cantidad de dispositivos. Estos últimos instalan los datos de las personas en la red.

Consignó que se debe buscar la protección adecuada de la información que es invisible. Detalló que en las redes de internet, solo el 5% de los datos son visibles.

Luego, destacó que las empresas y usuarios solo van a adoptar tecnologías en las que confían. Agregó que la actual normativa legal debe ajustarse a los estándares internacionales, en particular a los estándares planteados por la OCDE y, al mismo tiempo, ser coherentes con el ordenamiento jurídico local vigente.

Precisó que se debe asegurar el adecuado nivel de protección para los titulares, así como el incentivo al emprendimiento, la innovación y la competitividad del país. Añadió que, además, se debe contar con una institucionalidad moderna y eficiente.

Hizo presente que los temas principales a tratar en esta ley dicen relación con:

1.- Alcance y aplicación del proyecto de ley

2.- Definiciones, principios y derechos

3.- Consentimiento

4.- Tratamiento automatizado de datos

5.- Intermediario tecnológico

6.- Transferencia internacional de datos

7.- Infracciones y sanciones.

A continuación, **el Presidente de la Comisión, Honorable Senador señor Harboe**, ofreció la palabra **al Director legal de ACTI, señor Alex Pessó**.

El señor Pessó indicó, en cuanto al alcance y aplicación del proyecto de ley, que este tipo de legislaciones dicen relación con la administración de una base de datos y sobre los derechos y obligaciones que de ella emanan.

Agregó que la iniciativa presentada por el Ejecutivo trae una diferencia en el planteamiento, que consiste en que los derechos y obligaciones van más allá de la administración de una base de datos. Detalló que en la legislación europea, pronta a regir a partir de mayo de 2018, existe una diferenciación entre una base de datos y los derechos y obligaciones que ello conlleva.

Estimó que se debe revisar con mayor detalle si la mencionada diferenciación se recoge de manera adecuada, porque lo que se busca es certeza jurídica y lograr que el interesado sepa ante quién deba recurrir.

A raíz de lo anterior, manifestó que resulta importante hacer precisiones respecto a la diferencia que existe entre los conceptos de dato e información y cómo nos aseguramos que no se restrinja el derecho de emitir opinión y la libertad de expresión.

Luego, indicó que la Asociación que representa tiene sugerencias respecto a ciertas definiciones, como son las siguientes:

1) Dato personal: La definición del proyecto de ley debe ser complementada en relación a los medios que se utilicen para identificar a la persona; los cuales deben ser lícitos. Por otra parte, cabe destacar que no son sinónimos la palabra información con el término dato, siendo el primero más amplio que este último.

La sugerencia de la Asociación consiste en mejorar la definición de dato personal con el siguiente texto: Dato personal: es todo aquél que permita identificar con certeza a una persona natural, a través del uso de medios lícitos y esfuerzos razonables por parte del responsable.

2) Definición de dato sensible : Sigue siendo una definición muy amplia, con lo cual todo pasa a ser un dato sensible, por

cuanto todo dato personal se refiere a las características morales o físicas de una persona y todo dato podrá ser utilizado para discriminar a una persona. Debieran contemplarse casos concretos taxativos.

3) Definición de Responsable: Presentaría dos problemas: a) No circunscribe al responsable a la decisión sobre una “base de datos” y b) Independiza a dicho carácter de la “localización”.

a.- Si el concepto de responsable no está asociada a una base de datos, su definición resulta extremadamente amplia, e imprecisa. Esta situación nos enfrenta, agregó, a un escenario de incerteza jurídica que debemos relacionarlo a la potestad normativa que se le dota a la Agencia de Protección de Datos.

b.- La ley no puede pretender ir más allá de las fronteras. La ley solo puede regular las actividades que se produzcan en el territorio. Lo que sí puede exigir es que la exportación o circulación transfronteriza de datos se haga de manera segura y bajo ciertos estándares (ej. la “adecuación” internacional)

4) Definición de titular de datos: Atendida la amplitud de la definición incorporada en la Moción, se recomienda que se rechace dicha definición de titular de datos, y se opte por elaborar un nuevo concepto.

5) Definición de consentimiento: Es un avance en esta materia la nueva definición de consentimiento, que establece expresamente el Mensaje.

Sostuvo que el proyecto de ley del Ejecutivo incorpora nuevas definiciones en materia de derecho de acceso, derecho de rectificación, derecho de cancelación, derecho de oposición y derecho a la portabilidad de los datos personales.

Recomendó incorporar a cada una de las definiciones de los derechos del titular de los datos, la frase “del responsable de una base de datos”, para que quede claro, que los derechos deben ser ejercidos por los titulares de datos, frente a los responsables de las bases de datos.

En relación a los principios, explicó que el Mensaje incorpora un artículo 3°, con los principios, que deben aplicarse al tratamiento de datos.

Señaló que proponen en la definición de principio de seguridad agregar la expresión: “en forma razonable”, y eliminar la

referencia al “daño accidental” e incorporar la frase “dentro de las posibilidades de cada responsable de base de datos”.

Afirmó que daño accidental equivale a incorporar responsabilidad por el caso fortuito, lo que es contradictorio a nuestro ordenamiento jurídico.

En cuanto a los derechos, manifestó que el derecho de oposición, está redactado en forma tan amplia, que terminará afectando y colisionando garantías constitucionales de terceros. Así la letra (a) permite oponerse cuando el tratamiento de datos afecte derechos y libertades fundamentales. Esta restricción es tan amplia que un operador debe asumir que el titular siempre tendrá derecho a oponerse al tratamiento.

Sugirió establecer que no se aceptará oposición cuando el tratamiento sea necesario para ejercer el derecho a las libertades de emitir opinión y de informar, no limitado a los medios de comunicación social, sino que aplicable a todos los habitantes de la República de Chile.

En relación al tratamiento automatizado de datos, hizo presente que recomiendan evitar términos ambiguos como: “de manera significativa”, que podrían obstaculizar el tratamiento automatizado de datos personales.

Luego, agregó que resulta imprescindible distinguir claramente entre aquellas decisiones que produzcan efectos jurídicos negativos o afecten significativamente al titular de los datos y aquellos que no, y se centre, única y exclusivamente, en los primeros, para evitar que tratamientos automatizados como los arriba descritos se vean perjudicados y sometidos al mismo escrutinio y restricciones que aquellos otros tratamientos que pueden entrañar riesgos y perjuicios reales al ciudadano.

En cuanto a la Agencia de Protección de Datos, remarcó que la iniciativa en estudio establece una institucionalidad equilibrada. Agregó que ciertas sanciones que se consagran pueden resultar muy gravosas para ciertos segmentos empresariales. Apoyó la creación de la misma y expresó que ella debe avanzar de manera tal que Chile pueda contar con un adecuado nivel de protección de sus datos.

A continuación **el Presidente de la Comisión, Honorable Senador señor Harboe**, ofreció la palabra al **Secretario General de la Cámara de Comercio de Santiago, señor Cristián García Huidobro**.

El señor García Huidobro comenzó su presentación señalando que Chile cuenta con una normativa en esta materia desde el año 1999. Agregó la evolución de los últimos tiempos hace recomendable modernizar y poner a la altura del mundo desarrollado lo

relativo al tratamiento de los datos personales. En este sentido, señaló que compartía los lineamientos generales del proyecto.

Expresó que una normativa como la que se propone permitirá que los titulares de datos transiten del mundo de la desconfianza al de la confianza, sintiéndose con mayor propiedad y control sobre sus datos, de manera que libremente decidan entregar su información y permitan al comercio conocer a sus clientes para entregarles un mejor servicio.

Dicho lo anterior, consideró que hay materias que admiten ser perfeccionadas, así como hay otras que requieren precisiones.

La Cámara de Comercio de Santiago considera fundamental que el marco normativo contemple los siguientes elementos:

1. Equilibrio adecuado entre la protección de la privacidad de las personas y la libre circulación de la información.

A. Principio Rector

Sostuvo que el principio rector en materia de protección de datos es que los datos personales pertenecen al titular, por lo que la legislación debe garantizar el derecho de las personas de protegerlos y controlarlos.

Agregó que una ley de protección de datos debe otorgar las herramientas a los titulares para controlar su información sin obstaculizar la libre circulación de la misma para el desarrollo de las actividades comerciales y de otros órdenes.

Señaló que debe distinguirse entre el dato personal de un individuo, de la base de datos de la que pueda formar parte aquel dato personal. Así como el proyecto consagra -o reafirma- la propiedad exclusiva del dato personal en favor de su titular, la iniciativa también debiera consagrar en forma explícita la propiedad sobre la base de datos -como conjunto armónico- a su constructor.

Connotó que debe existir un equilibrio adecuado entre la protección de la privacidad de las personas y la libre circulación de la información.

B. Envío de Comunicaciones Comerciales

Indicó que es de público conocimiento que el aumento en el envío de la publicidad puede resultar invasivo, por lo que estimó positivo que se pretenda regular la materia.

Añadió que al exigir el consentimiento de los titulares el Mensaje cambia el sistema actual "*Opt Out*" al sistema "*Opt In*" en el cual se requiere consentimiento (expreso, previo, libre, especifico e informado) del titular de datos para el envío de comunicaciones comerciales. Ello dificulta el envío, perjudicando el desarrollo comercial principalmente de las empresas de menor tamaño.

Destacó que un modelo como el que establece el Mensaje, implica que las empresas de menor tamaño se verán forzadas a crear una estructura para obtener el consentimiento de los titulares de datos para poder enviar su publicidad. Estas exigencias constituirán obstáculos al emprendimiento y al flujo comercial. Propuso conservar el sistema actual "*Opt Out*", perfeccionándolo con la implementación de Listas de Exclusión Publicitaria certificadas por la Autoridad de Protección de Datos. En el mismo sentido está planteado el proyecto de ley Boletín N° 10.791, de los Honorables Senadores Bianchi, Prokurica, Tuma y Guiller que ingresó a tramitación en Julio del año 2016 e incorpora nuevos incisos al artículo 28 B de ley N° 19.496 Sobre Protección de los Derechos de los Consumidores. En efecto, dicha moción mantiene la modalidad actual de envío de comunicación comercial o publicitaria, pero incorpora la idea de un registro "No Molestar" gratuito para el consumidor y que obliga al proveedor a abstenerse de enviar comunicación promocional o publicitaria a quien este incorporado en el registro. Asimismo, se limita el día y la hora para la comunión vía telefónica.

Aseveró que la mayor parte de la legislación comparada ha solucionado este problema implementando listas de exclusión publicitaria, conocidas como "Listas Robinson" en España, "*Do Not Call*" en U.S.A, y "No Molestar" en México y Argentina.

Precisó que de esta forma se logra una efectiva y real protección de los derechos de los consumidores, y al mismo tiempo se permite el legítimo derecho de dar a conocer sus productos a las empresas. Así se respetaría la libertad personal, permitiendo a los titulares de los datos decidir cuál comunicación quieren recibir y cuál no.

Añadió que si es que se decide cambiar al sistema "*Opt In*", según lo plantea el Mensaje, será necesario compatibilizarlo con lo establecido en el artículo 28 letra B de la ley N°19.496 sobre protección de los consumidores que regula la comunicación promocional o publicitaria enviada por correo electrónico.

C. Comercio Electrónico y Protección de Datos

Manifestó que la protección de datos es un aliciente para mejorar la confianza de los consumidores en el uso de Internet como canal de comercialización. Ésta debe ser acorde con el estándar internacional a los efectos de lograr coherencia regulatoria con los entornos de referencia de Chile.

Expuso que es indispensable nivelar la cancha con los actores del comercio electrónico internacional, sobre todo por el hecho de que éste no respeta fronteras. Para ello, la Cámara de Comercio de Santiago considera que se debe hacer aplicable la legislación chilena a los proveedores extranjeros, con independencia de si se encuentran establecidos en Chile, en la medida que los bienes o servicios ofertados estén destinados a personas domiciliadas en el país.

2. Existencia de una Autoridad de Protección de Datos

Consideró como fundamental que el Mensaje considere la incorporación de una autoridad de protección de datos, que vele por el cumplimiento de la normativa, aplique sanciones siguiendo un procedimiento sancionatorio previamente establecido y ejerza las funciones que la ley le faculta técnicamente. Sin embargo, aseguró que tal como está concebido en el proyecto de ley se presentan los siguientes problemas:

A. Autonomía e Independencia

La Agencia de Protección de Datos se contempla como un organismo público, descentralizado, con personalidad jurídica y patrimonio propio, sometido a la súper vigilancia del Presidente de la Republica a través del Ministerio de Hacienda. La dirección y administración superior de esta institución estará a cargo de un Director (a) nombrado exclusivamente por el Presidente de la Republica conforme al sistema de Alta Dirección Pública.

Sostuvo que la independencia y autonomía son valores consustanciales a la institución de la Autoridad de Protección de Datos y un común denominador a dicha entidad en la legislación europea.

Consideró que la manera de alcanzar dichas independencia y autonomía depende de los mecanismos de nombramiento y de remoción de quien o quienes tienen a su cargo la dirección y administración de la Agencia de Protección de Datos. La estructura de dirección y administración de la Agencia de Protección de Datos propuestas en el Mensaje parecieran no alcanzar los estándares de la normativa internacional en esta materia.

Connotó como más adecuado que en lugar de un órgano unipersonal, se considere un órgano colegiado de fisonomía técnica, dedicación exclusiva e integración pluralista.

Sostuvo que este órgano pluripersonal debiera estar integrado por, a lo menos, tres miembros designados por el Presidente de la República con acuerdo previo de 2/3 del Senado. Estos miembros deberían permanecer en el ejercicio de sus funciones un período de 8 años y cesar en ellas por el término del periodo referido o por causales establecidas taxativamente en la ley con el informe favorable de la Corte Suprema. (Renuncia voluntaria aceptada por el Presidente de la República, destitución, por negligencia manifiesta, en el ejercicio de sus funciones, Incapacidad).

Agregó que en caso de desecharse una composición colegiada en la dirección de la Agencia y mantenerse la estructura de administración y dirección que contempla el proyecto de ley, es fundamental que el nombramiento y remoción del Director se efectué con las características señaladas en el párrafo anterior, con la finalidad de optimizar los niveles de independencia con respecto a otros poderes del Estado.

B. Incompatibilidades

En lo que dice relación con las incompatibilidades e inhabilidades para ejercer el cargo de Director o Directora, la iniciativa legal prohíbe que ocupen el cargo y que tengan participación en la propiedad de una empresa cuyo objeto o giro comercial verse sobre recolección, tratamiento o comunicación de datos personales tanto él/ella, como la/el cónyuge o conviviente civil del Director o Directora y sus parientes hasta el segundo grado de consanguinidad inclusive. La amplitud o extensión de esta norma de incompatibilidades es excesiva. Enfatizó que debe reconsiderarse este tema.

3. Derecho de los Titulares

A. Derecho de Acceso

De acuerdo a los registros de la Cámara de Comercio de Santiago, en el Boletín de Informaciones Comerciales, los titulares de datos ejercen el derecho de acceso, en promedio, una vez al año. Por lo tanto estimó suficiente mantener la legislación actual que contempla el ejercicio del derecho de acceso gratuito semestralmente.

B. Procedimiento de Tutela de Derechos de los Titulares

El Mensaje establece que la Autoridad de Protección de Datos conocerá el procedimiento de tutela de derechos de los

titulares de datos. En caso de vulneración de sus derechos por un órgano público se contempla una reclamación de ilegalidad ante la Corte de Apelaciones, sin pasar por la Agencia de Protección de Datos. A consecuencia de ello frente a una misma vulneración de derechos, pueden resultar sanciones diferentes según sea la categoría del autor. El costo monetario será mayor si la transgresión la produjo un organismo público, lo que parece poco presentable.

4. Principios para el Tratamiento de datos y Obligaciones para los Responsables de las Bases de Datos

Los principios implican obligaciones concretas para los responsables del tratamiento de datos que están definidas en el Mensaje:

i. Deber de secreto y confidencialidad

ii. Deber de información y transparencia

iii. Deber de adoptar medidas de seguridad

iv. Deber de reportar vulneraciones a las medidas de seguridad.

Agregó que las empresas deberán incurrir en los costos necesarios para cumplir con estas obligaciones lo que unido a eventuales sanciones puede afectar la continuidad de sus operaciones.

Subrayó que ante dicho riesgo, debe establecerse un período de marcha blanca para la aplicación de sanciones.

5. Régimen de Infracciones y Sanciones

El Mensaje contempla multas hasta UTM 5.000. Consignó que éstas son excesivamente altas considerando normativas de similar naturaleza que esta misma Comisión del Senado está estudiando.

Sostuvo que también se contemplan multas que pueden alcanzar las UTM 15.000 cuando hay reincidencia, entendiéndose por tal 2 o más sanciones ejecutoriadas en un período de 24 meses, cualquiera sea la identidad de la infracción. Estimó que la reincidencia debiera consistir en la reiteración de una misma conducta.

Asimismo, manifestó que siguiendo la tendencia legislativa se debe incorporar un tope máximo de las multas el que no debiera exceder del 15% de las ventas correspondientes al mes en que se cometió la infracción. Si la infracción se extendiera por más tiempo, dicho

porcentaje se aplicaría sobre las ventas de todo el período por el que se prolongó.

Indicó que el régimen de infracciones contempla sanciones accesorias como la suspensión de la operación de tratamiento de datos hasta por seis meses y, en caso de persistir el incumplimiento, la empresa responsable de la base de datos no podrá volver a desarrollar actividades de tratamientos de datos personales.

Considerando que una misma empresa puede operar dos o más bases de datos, la sanción sea de suspensión o de inhabilitación debiera aplicarse a la base en que se cometió la infracción, sin afectar a las otras bases de datos.

En materia de sanciones también llama la atención la paradoja de que las accesorias, como son la suspensión e inhabilitación, pueden resultar más perjudiciales a las empresas que las sanciones principales (Multas).

Sostuvo que las anotaciones en el Registro de Sanciones se mantendrán por 5 años. Esta sanción también puede resultar desmedida en relación a la inconducta, por lo cual sugirió establecer plazos proporcionales a la gravedad e impacto de la infracción y a la actitud del infractor.

6. Excepciones al Consentimiento

En el Mensaje se establece que es lícito el tratamiento cuando el consentimiento del titular es libre e informado, específico en relación a la finalidad y que debe otorgarse en forma previa. El texto establece como excepciones a la exigencia de consentimiento del titular:

a) Cuando el tratamiento se refiere a datos personales que han sido recolectados de una fuente de acceso público,

b) Cuando el tratamiento este referido a datos de carácter económico, financiero, bancario y comercial realizándose de conformidad con las normas del título III de esta ley y;

c) Cuando el tratamiento es necesario para cumplimiento de una obligación legal o contractual de que es parte el titular de tales datos.

Consideró correctas las citadas excepciones, sin embargo, estimó que es importante agregar las siguientes:

- Datos personales tratados por Órganos del Estado en el ejercicio de su competencia y en la forma prescrita en la ley.

- Cuando los datos sean tratados para proteger la vida del titular.

- Cuando el tratamiento de datos sea utilizado exclusivamente para *marketing* directo o comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes y finalmente,

- Para tratamientos de datos precontractuales.

7. Responsable de Datos y Encargado de Datos

Explicó que el Mensaje define lo que se entiende por responsable de datos, pero no ocurre lo mismo con encargado de datos. Señaló que el responsable y encargado no necesariamente son iguales. En consecuencia, se mostró partidario de incorporar la definición del encargado de datos y establecer claramente las responsabilidades que en las gestiones corresponde a cada uno de estos actores.

8. Modelo de Prevención de Infracciones

Añadió que esta iniciativa regula un incentivo para el cumplimiento de la normativa estableciendo modelos de prevención de infracciones que, cuando estén certificados, serán considerados como atenuantes de responsabilidad. La Agencia de Protección de Datos será la encargada de certificar que el modelo y programa de cumplimiento reúne los requisitos y elementos establecidos en la ley y de supervisarlos. La certificación dura hasta 3 años.

Aseveró que comparte la idea expresada en el proyecto, pero consideró como más conveniente que la referida certificación sea practicada por terceros previamente acreditados ante la Agencia de Datos.

9. Indemnización de Perjuicio

El tema de la responsabilidad civil está regulado en el artículo 51 del Mensaje. Estimó como esencial establecer que las acciones indemnizatorias de perjuicios se deben interponer en sede civil y que la Agencia de Protección de Datos no tiene facultades jurisdiccionales para conocer de las mismas, sino solo determinar infracciones e imponer sanciones.

A continuación, se refirió a las ideas contenidas Moción sobre protección de datos personales (Boletín N° 11.092).

Manifestó que ella contiene aspectos positivos cuya incorporación en el texto de esta última podría enriquecer la normativa que en definitiva se despache por el Congreso Nacional.

Desde el punto de vista formal, la Moción propone consagrar una nueva ley que derogue y reemplace a la actual ley N° 19.628. Definitivamente se inclina por perfeccionar y modernizar la legislación existente en materia de protección de datos, siguiendo el sendero delineado por el Mensaje, en vez de sustituir un cuerpo legal por otro, ya que se corre el riesgo de que éste último no cubra adecuadamente todos los aspectos y ámbitos de la protección de datos personales.

Hizo presente que los aspectos positivos de la Moción son los siguientes:

1. Envío de Comunicaciones Comerciales

La Moción, en esta materia reconoce el sistema actual de envío de publicidad incorporando el concepto de listas de exclusión publicitaria, al consagrar el derecho a oponerse al tratamiento de datos cuando estos son utilizados para comunicaciones comerciales o publicitarias y el titular se ha incluido en algún registro público o privado de exclusión publicitaria, lo que nos parece un criterio acertado, tal como lo señalamos en un capitulo anterior de esta presentación.

2. Sanciones

Se mostró de acuerdo en que las sanciones consistentes en multas tengan un límite o tope máximo que prevenga la posibilidad de que tal multa pueda significar la insolvencia o disolución de la empresa. De allí que es positivo que dicho tope máximo diga directa relación con las ventas del infractor. Por ello, tal como lo señaló anteriormente resulta esencial incorporar un tope máximo de las multas el que no debiera exceder del 15% de las ventas correspondientes al mes en que se cometió la infracción. Si la infracción se extendiera por más tiempo, dicho porcentaje se aplicaría sobre las ventas de todo el período por el que se prolongó.

3. Fuente de Acceso Público

En lo que respecta a la fuente de acceso público, indicó que la Moción se encarga de definir lo que se entiende por ella y señala taxativamente cuáles son, lo cual parece adecuado.

Concluyó señalando que sería preferible que tan importante concepto quede definido en la ley, para prevenir discrecionalidades en el campo administrativo.

A continuación, **el Presidente de la Comisión, Honorable Senador señor Harboe,** ofreció la palabra a los miembros de la Comisión con la finalidad de que formulen preguntas o hagan observaciones a las exposiciones efectuadas.

En primer lugar, hizo uso de la palabra el **Honorable Senador señor Larraín,** quien señaló que compartía la inquietud formulada respecto de la Agencia de Protección de Datos, como organismo dependiente del Ministerio de Hacienda.

Agregó que hay que tener especial cuidado en el ámbito de la información, porque cualquiera sea el organismo público que se haga cargo de dicha función, en la medida que sea parte del Ejecutivo, tendrá una connotación política, por más técnica que resulte su actividad.

Recalcó que así lo han hecho saber distintos sectores de la industria. Por lo mismo preguntó a los representantes del Ejecutivo ¿cómo se regula y organiza este tipo de Agencia en el ámbito internacional?.

Sostuvo que la concepción de la separación de los poderes públicos está sobrepasada y ya no responde a la realidad. Actualmente la estructura de organización del poder tiende a buscar cómo se va delimitando de acuerdo a la forma como éste actúa.

Añadió que una manera efectiva de lograr el buen funcionamiento de estos organismos es mediante la creación de órganos autónomos e independientes. Ejemplificó con lo que ha sucedido con el Banco Central.

Luego, destacó que estamos en un espacio en donde una excesiva injerencia de la autoridad en los datos personales, no ayuda al desarrollo adecuado de esta materia.

Asimismo, resaltó la necesidad de buscar un cierto equilibrio entre la libre circulación de la información, versus el resguardo de los datos de las personas. Connotó que hay un espacio de protección de los derechos de las personas que debe ser amparado.

Remarcó que junto a otros Senadores ha promovido una agenda muy potente de acceso a la información pública. Enfatizó que Chile es un modelo de lo anterior. Lo ejemplificó con el Consejo para la Transparencia. Aseveró que se está promoviendo legislación de

acceso a la información o de obligación de organismos privados que deben dar alguna información, porque en este último ámbito hay antecedentes que deben ser públicos.

Asimismo, solicitó que los expositores profundicen los conceptos de “*Opt in*”, “*Opt out*”.

Expresó que uno de los invitados señaló que “la ley no puede ir más allá de las fronteras”. Preguntó por la empresa Alibaba y si ésta pagaba los impuestos correspondientes, tal como lo hacen las empresas del *retail* instaladas en nuestro país. Consultó cómo se puede regular lo planteado.

En relación a las sanciones, manifestó que el régimen actual no ha sido eficaz para impedir los abusos de los datos personales, particularmente en el traspaso de base de datos. Preguntó ¿cómo puede alguien que está en la mencionada base evitar ser parte de una transacción? Consultó ¿cómo, en definitiva, se evita el tráfico de datos?

Aseveró que lo planteado no ha sido abordado por la actual legislación y ratificó que estamos en presencia de temas complejos.

En seguida, **el Presidente de la Comisión, Honorable Senador señor Harboe,** sostuvo que en el debate ha advertido una especie de contradicción entre la libertad del ciudadano para poder permitir que alguien le envíe información y la protección de datos. Consideró que en ello no hay incompatibilidad. Agregó que la libertad del ciudadano se mantiene cuando no se ve invadido por publicidad que no ha solicitado.

Agregó que el sistema no está funcionando. Recalcó que las intromisiones incluyen los diversos medios de comunicación, incluyendo *whatsapp*.

Asimismo, hizo presente que la ley N° 19.628, que está completamente superada, pudo en el pasado haber otorgado protección, pero en la práctica se dedica a administrar el tratamiento más que proteger los derechos de las personas.

Consideró también necesario efectuar un análisis de la institucionalidad, pero ello no constituye la discusión principal de la iniciativa. Destacó que cada vez que logramos identificar una falencia de política pública se intenta crear una nueva institucionalidad. Se mostró partidario de la estructura consecuencial, es decir, que ellas, ya sean privadas o públicas, deben ser el resultado de un objetivo que busca un determinado tipo de legislación.

Manifestó que uno de los puntos a considerar en la discusión en particular, consiste en la información que tiene el carácter de utilidad pública. Sostuvo que en Chile, los organismos de emergencia carecen de potestad pública para poder requerir información para enfrentar determinado tipo de situaciones. Señaló, por ejemplo, los incendios con productos químicos donde bomberos no cuenta con la información adecuada para poder llegar de manera oportuna y con el equipo suficiente para atender la emergencia.

Precisó que lo mismo sucede con las instituciones de seguridad. Ellas deben estar dotadas de la potestad legal para poder requerir cierta información a determinadas empresas.

Asimismo, indicó que la capacidad de mantener los niveles de seguridad requiere del trabajo y de la coordinación de la información. Agregó que los países que han alcanzado un mejor resultado en la mencionada materia, son aquellos que han logrado tener motores de búsqueda que permiten comparar un conjunto de información que generan patrones predictivos o acciones focalizadas.

Mencionó que un segundo punto dice relación con los datos comerciales. Sostuvo que si hay algo que afecta a los ciudadanos es el tráfico de información comercial. Recordó que el decreto supremo N° 950 del Ministerio de Hacienda, del año 1928, le entrega a la Cámara de Comercio la administración del boletín comercial. Lo anterior, indicó, la transforma en una institución privilegiada respecto del resto del mercado.

Reconoció que existen instituciones privadas que trabajan con datos comerciales de las personas. Añadió que éstos son transferidos y cedidos sin que los ciudadanos sean consultados. Lo anterior produce una situación de asimetría y de afectación de derechos.

Consignó que cuando se producen ventas, fusiones y adquisiciones de empresas, también se incorporan a ella, los datos. Se preguntó si en esos casos alguien consulta al titular de dichos datos. Esta situación, ejemplificó, se produce cuando una cadena farmacéutica es adquirida por una compañía de seguros.

Asimismo, hizo presente la situación que se da con los exámenes de ADN. Esto último corresponde a un dato, un registro. Inquirió qué sucedería si las personas se realizan exámenes preventivos de ADN, para saber eventuales prevalencias. Qué pasaría si esa información es vendida a compañías de seguros.

Valoró la opinión de los expositores en cuanto a la necesidad de tener una nueva legislación. Aseveró que es la oportunidad de

aprovechar esta instancia de discusión para hacernos cargo de desafíos que vienen.

Seguidamente, **la Coordinadora de Finanzas Internacionales y Mercado de Capitales, del Ministerio de Hacienda, señora Bernardita Piedrabuena**, señaló que hoy en día la ley N° 19.628 es poco eficaz, ya que pocos la cumplen y es por ello que se produce el tráfico de bases de datos y se vulneran los derechos de las personas. Lo anterior, continuó, se produce porque no hay una Agencia, ni un ente regulador que vele por el cumplimiento de ese cuerpo legal.

Enfatizó que la protección de los datos personales constituye un derecho fundamental y así quedará consagrado con la reforma constitucional que se encuentra en segundo trámite legislativo. El mencionado derecho se contrapone al de transparencia. Agregó que el Consejo para la Transparencia y la Agencia de Protección de Datos son quienes deben intentar solucionar el conflicto que se produzca entre ambos, y si ello no sucede, son los tribunales de justicia los llamados a resolverlo.

Agregó que el Ejecutivo viene en proponer la Agencia de Protección de Datos pero no como organismo autónomo. Aseveró que el Consejo para la Transparencia constituye una anormalidad dentro de la institucionalidad chilena, ya que los organismos fiscalizadores, por regla general, no son autónomos. Recalcó que cuestión distinta es la independencia, y esta última se alcanza a través de distintos mecanismos, como son, por ejemplo, el nombramiento de sus integrantes.

En seguida, **el Presidente de la Comisión, Honorable Senador señor Harboe** ofreció la palabra **al Presidente de la Asociación Chilena de Empresas de Tecnología de Información A.G., señor Raúl Ciudad**.

El señor Ciudad respondiendo a la pregunta sobre la empresa *Alibaba*, señaló que la mencionada compañía, cuando vende un producto, deja en manos del comprador la decisión de pagar los impuestos.

En relación a la empresa *Uber*, expresó que el desafío es modernizar nuestra legislación para controlar a compañías que operan en Chile con nuevos modelos tecnológicos.

Añadió que los datos sensibles deben estar adecuadamente protegidos. Por lo tanto, el desafío es definir qué es un dato público y qué entenderemos por dato privado o sensible. Apuntó que aquellos que se encuentran en las fichas clínicas corresponden a estos últimos. Remarcó que el ADN es un dato altamente sensible, porque a través de él se puede determinar las enfermedades que cada persona padecerá.

Seguidamente, **el Director legal de ACTI, señor Alex Pessó** consignó que en general para las empresas estas materias constituyen un factor más de la competitividad. Detalló que en Estados Unidos de Norteamérica se aplica el principio de usos y obligaciones, en donde lo que importa es cómo se utilizan los datos. Es allí donde se debe poner atención.

Aclaró que en el mundo de hoy se recolectan datos permanentemente. Explicó que esta situación no es necesariamente negativa para el ciudadano, sino que también puede implicar un beneficio.

Finalmente, **el Secretario General de la Cámara de Comercio de Santiago, señor Cristián García Huidobro,** manifestó que hace dieciocho años que la ley autoriza que se creen boletines comerciales, y durante ese lapso de tiempo no se ha creado ninguno.

En la sesión siguiente, el **Presidente de la Comisión, Honorable Senador señor Harboe**, ofreció la palabra a **los representantes de la empresa Equifax, señores Ignacio Bunster y Carlos Johnson.**

El Gerente General, señor Carlos Johnson agradeció la invitación cursada por la Comisión a exponer en el presente proyecto de ley. Reconoció que para Equifax constituye una gran oportunidad poder realizar observaciones a la presente iniciativa. La consideró de gran relevancia, atendido el giro de la compañía. Apuntó que pueden contribuir a la iniciativa, gracias a la experiencia que han adquirido en otros países donde operan.

Agregó que la empresa nació hace 120 años y está presente en más de veinte países.

A continuación, hizo uso de la palabra **el Director Legal** de esta empresa**, señor Ignacio Bunster** quien manifestó que estamos ante una oportunidad única para reformular la normativa sobre protección y tratamiento de datos personales que permita, no solo ubicar a Chile al nivel de otras legislaciones modernas sino, además, ir un paso más allá y reconocer en la nueva ley las nuevas tecnologías, tendencias y oportunidades que actualmente existen y que marcarán el futuro en esta materia. En este sentido, estimó que la ley que se dicte debe sostenerse sobre los siguientes pilares fundamentales:

a. Más Datos: El acceso a una mayor profundidad y completitud de datos permitirá hacer mejores evaluaciones lo que redundaría en menores costos, mayor acceso al crédito y, en definitiva, mayor inclusión financiera. La falta de información, por el contrario, impide distinguir entre buenos pagadores y malos pagadores; entre quienes tuvieron

un problema económico puntual y quienes consistentemente no pagan sus deudas; entre quienes se endeudan responsablemente y quienes están sobre-endeudados.

b. Mejores Datos: Además de una mayor cantidad de datos, éstos deben ser completos, fidedignos y exactos, con un marco que establezca claramente (i) los derechos de los titulares de datos respecto del manejo de los mismos por parte de terceros, y (ii) la responsabilidad de todos quienes traten dichos datos personales de modo de asegurar que éstos entreguen información lícita, veraz y valiosa para los procesos de evaluación.

c. Data Positiva: En este contexto, consideró como fundamental que la nueva normativa regule expresamente el tratamiento de información positiva. Destacó que Chile es uno de los pocos países en América Latina que aún no ha regulado el uso de este tipo de información.

d. Inclusión Financiera: Todo lo anterior es el medio para alcanzar una mayor inclusión financiera. El acceso al crédito, la rebaja en los costos y tasas de interés será consecuencia de poner a disposición del mercado más y mejores datos.

e. Regulación: Para que este fin se cumpla es necesario un conjunto de reglas claras, una entidad con facultades para exigir su cumplimiento y con herramientas para sancionar su vulneración y actores responsables que entiendan el valor de los datos personales y la urgencia de su respeto y protección. De este modo, no solo es necesaria una nueva y más robusta ley y una autoridad que la sirva y aplique sino también responsables del tratamiento de datos que se autorregulen y un mercado que no tolere, ni por acción ni por omisión, la piratería de datos.

f. Titularidad del Consentimiento como principio rector de la normativa sobre protección y tratamiento de datos personales: Al alcanzar la mayoría de edad, nuestro ordenamiento jurídico entrega a las personas el derecho a elegir a las autoridades que regirán el destino del país, contraer matrimonio, conducir, entre otros muchos derechos y obligaciones. No obstante lo anterior, esta ley, y la normativa sobre protección de datos en general, considera que no hay edad suficiente para considerar a las personas capaces para disponer de datos que son de su propiedad. En opinión de EQUIFAX, cada titular debiera ser responsable y soberano, sin restricciones, de disponer del destino de sus datos, haya o no respecto de ellos la especificidad que la definición de consentimiento exige.

Entrando en el análisis particular del proyecto de ley, manifestó que en cuanto a la definición de fuentes de acceso público, es partidario de la línea seguida en la iniciativa del Ejecutivo, donde se definen las fuentes. Criticó que en la Moción se señala un número muy acotado de

ellas, lo que puede resultar perjudicial si el día de mañana surgen nuevas. Añadió que basta pensar lo que ha pasado desde el año 1999, en que se dictó la ley vigente sobre datos personales, e imaginar qué hubiese sucedido si en el mencionado cuerpo legal se hubiesen enumerado las fuentes que estaban disponibles. Se preguntó qué hubiese ocurrido con las nuevas fuentes de acceso público que surgieron en el período intermedio.

En relación al principio de finalidad, consideró como fundamental que exista y que esté claramente definido. Destacó que el enfoque presente en ambos proyectos de ley pone el énfasis de manera casi exclusiva en la protección de los datos y la propiedad de los mismos por parte de sus titulares, afectando la generación de nuevas oportunidades y análisis a partir de los mismos datos. Lo anterior, afirmó, provoca un desincentivo a la actividad económica.

En cuanto al principio de proporcionalidad y temporalidad, estimó que establecen elementos de subjetividad que pueden no ser muy convenientes. Agregó que establecer la necesidad, relevancia, oportunidad o adecuación de datos será materia que debe ser resuelta por la Agencia de Protección de Datos, caso a caso. Sostuvo que en opinión de EQUIFAX, la vigencia y relevancia de los datos personales subsiste en el tiempo y ella es la que, muchas veces, entrega la información más valiosa al describir comportamientos a través del tiempo.

Consignó que respecto a la licitud del tratamiento, en la Moción se señala que éste es lícito, entre otras hipótesis, cuando intereses legítimos perseguidos por el responsable del tratamiento o por un tercero no entran en colisión con los intereses, derechos y libertades fundamentales de los titulares de datos. Connotó que establecer un mecanismo que por la vía administrativa dirima las controversias, le restará efectividad a la ley.

Respecto al derecho de oposición, expresó que el artículo 8° del Proyecto del Ejecutivo establece este derecho y los casos en los cuales aplica, incluyendo en su párrafo b): “Cuando el tratamiento de datos sea utilizado exclusivamente con fines de marketing directo de bienes o servicios, así como cualquier otro propósito comercial o fines publicitarios, salvo que exista un contrato entre las partes que expresamente contemple dicho uso de su información”. Debe tenerse presente que dicha hipótesis es una de las excepciones al consentimiento contenidas en el artículo 4° de la Ley 19.628.

Añadió que la redacción actual ubica este caso dentro del sistema “*Opt Out*”, lo cual parece adecuado, sin embargo, se le excluyó del listado de excepciones al consentimiento contenido en el artículo 13 del Mensaje. De cierta forma las comunicaciones de *marketing* directo quedan en una cierta tierra de nadie. Estimó positivo para el desarrollo del

comercio que este tipo de comunicaciones se mantenga dentro de las excepciones al consentimiento pero poniendo, a disposición de los titulares de datos, un mecanismo claro y efectivo para ejercer el "*Opt Out*".

Propuso la creación de un mecanismo que siga alguna de las experiencias exitosas que actualmente existen a nivel internacional como las listas Robinson de exclusión publicitaria que se utilizan en España. Esto permitirá dar adecuada protección a los derechos de los titulares de datos sin imponer trabas excesivas al comercio.

En cuanto al Tratamiento Automatizado de Datos Personales, relató que en ambos proyectos de ley existen numerosas referencias a este concepto. En los tiempos del *Big Data* y el *Cloud Computing* es difícil imaginar un tratamiento de datos que no sea automatizado. Sin embargo, en ambos proyectos se percibe una aproximación negativa a este concepto.

Especificó que en ellos se señala que los titulares tienen derecho a solicitar al responsable que ninguna decisión que les afecte de manera significativa se adopte exclusivamente basada en el tratamiento automatizado de sus datos que ofrezca una definición de sus características

Manifestó que lo que subyace al concepto es cierta desconfianza hacia la elaboración de perfiles, modelos, scores y otros análisis de los titulares construidos a partir de su información personal.

Añadió que lo que parece estar detrás de estos preceptos es una desconfianza hacia la elaboración de perfiles, modelos, scores y otros análisis de los titulares construidos a partir de su información personal. Se les relativizaría su valor como herramienta predictiva y se les limitaría en su aplicación. Lo anterior parece quedar confirmado con lo dispuesto en la Moción, la cual, en su artículo 16°, párrafo e) permite ejercer el Derecho de Oposición "cuando los datos sean usados para la elaboración de perfiles".

Hizo presente que el tratamiento automatizado de datos personales no solo es una realidad sino una necesidad; su alcance va mucho más allá de lo que se puede imaginar e interviene en procesos que, de otra forma, no podrían realizarse o serían ostensiblemente menos eficientes. Ejemplificó con el convenio de EQUIFAX con Carabineros de Chile a través del cual el Departamento especializado de Encargo y Búsqueda de Personas y Vehículos utiliza la data de la empresa que representa para hacer más eficiente la búsqueda de personas perdidas y vehículos robados. Afirmó que con ello se han logrado resultados concretos en menor tiempo.

En cuanto al tratamiento de datos relativos a obligaciones de carácter económico, financiero, bancario o comercial, opinó que la Moción introduce ciertas disposiciones nuevas que acarrean más perjuicios que los beneficios que intenta provocar. Al respecto, señaló lo siguiente:

i. El inciso 3° del artículo 22 adopta lo dispuesto en la parte final del inciso 2° del artículo 17 de la ley 19.628 al señalar que “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”.

Señaló que la norma original ya era inapropiada por lo que la incorporación de nuevas deudas excluidas agrava dicha situación. Lo que existiría en los hechos es una discriminación entre unos acreedores y otros, más que una protección ante el no pago de ciertas deudas por servicios más sensibles. Lo que es peor, esta norma iría en un sentido diametralmente opuesto a esfuerzos del Ejecutivo para frenar la evasión en el transporte público, por ejemplo, o a los más recientes pronunciamientos sobre la materia o recomendaciones normativas que apuntan a permitir la publicación de las morosidades asociadas a ciertos servicios considerados como básicos. Demás está decir que no se ve justificación alguna en mantener la excepción respecto de las deudas por uso de autopistas.

Connotó que no se deben establecer estas excepciones las cuales amparan conductas derechamente abusivas que afectan los negocios de las empresas afectadas y, como consecuencia, encarecen el servicio de los buenos pagadores. Más bien, se debe atender a la situación de las personas y profundizarse la prohibición asociada a la cesantía que podría afectar a los titulares de datos. La cesantía es una situación objetiva y demostrable y frente a ella consideró razonable la existencia de un tratamiento especial.

Añadió que el artículo 23 del proyecto de ley presentado por los Honorables Senadores recoge lo contenido en el Boletín 9.917-03, insistiendo en la necesidad de cancelarse los datos relativos a obligaciones pagadas o extinguidas por cualquier otro modo legal de extinguir las obligaciones sin requerimiento del titular, agregando que respecto de ellos se procederá, para todos los efectos legales, como si no hubieran existido jamás.

Recordó que con fecha 8 de marzo de 2017 la Comisión de Economía del Senado escuchó la opinión de expertos y actores relevantes en la materia (Superintendente de Bancos e Instituciones

Financieras, Coordinadora de Mercados de Capitales y Finanzas Internacionales del Ministerio de Hacienda, Presidente de la Cámara Chileno Norteamericana de Comercio, entre otros) respecto del referido Boletín, quienes coincidieron en la importancia de la data histórica y los beneficios de la misma para los solicitantes de crédito.

En relación a la Agencia de Datos, sostuvo que la tendencia mundial se ha inclinado por un órgano colegiado. Afirmó que con la finalidad de obtener una mayor autonomía e independencia, lo más aconsejable es que el mencionado organismo tenga dicha naturaleza.

Expresó que la distinción entre infracciones leves, graves y gravísimas parece adecuada, al igual que las situaciones descritas en cada categoría. Indicó que no les merece la misma opinión los criterios para determinar la cuantía de las multas, algunos de los cuales, atentan derechamente contra el principio de igualdad ante la ley. Constató que si las infracciones son objetivas también deben serlo los criterios, atenuantes o agravantes, que deban considerarse al momento de ser aplicados.

Estimó que las sanciones accesorias del Mensaje son excesivas; de hecho pueden llegar a ser más severas que la sanción principal. Apreció más razonable la sanción contenida en la Moción, en el cual la reiteración de infracciones muy graves acarrea la inhabilidad perpetua de la base de datos infractora. Añadió que el proyecto de ley del Ejecutivo inhabilita a perpetuidad a la entidad infractora, constituyéndose en un desincentivo desproporcionado a la actividad de tratamiento de datos.

Luego, explicó que la Moción introduce en su artículo 21 el concepto de interés colectivo cuyo alcance y conveniencia es, a lo menos, discutible. Lo anterior supone una intromisión del Servicio Nacional del Consumidor en el ámbito propio de la protección de datos personales, cuestión que fue objeto de larga discusión en su momento cuando se buscaba determinar qué autoridad debía tener bajo su control esta tarea y que se zanjó señalándose que el SERNAC no era la autoridad más idónea porque suponía rebajar los datos personales a la calidad de bien de consumo.

Hizo presente que un tema de gran relevancia quedó excluido de ambos proyectos, a saber, el de la *data positiva*. Ella ha demostrado a nivel mundial ser la mejor herramienta para la inclusión financiera. Agregó que Chile es uno de los pocos países que aún no la incorpora.

Apuntó que el Banco Mundial ha destacado expresamente la necesidad de que los registros de información crediticia incluyan información positiva. Señala que, como principio general, un sistema de información crediticia debe reunir información relevante, precisa, oportuna

y suficiente, para lo cual se ha de incluir información positiva además de la negativa. Por el contrario, reunir información inadecuada e incompleta conduce a numerosos problemas, incluyendo injustificados rechazos de créditos o aumento de los costos de los mismos.

Destacó que los beneficios que acarrea la información positiva son:

i. Crecimiento para la industria financiera;
ii. Mayor acceso al crédito;
iii. Un sistema de créditos más equitativo;
iv. Asignación de créditos más inteligente;
v. Crédito a más bajos costos; y
vi. Reducción de la pobreza y la creación de activos.

Consignó que estamos ante un momento único. Agregó que Chile tiene la oportunidad de situarse al nivel de las legislaciones más modernas en materia de protección de datos. Asimismo sostuvo que se pueden incluir en este proyecto de ley materias de gran relevancia y que suponen el reconocimiento de tecnologías, tendencias y oportunidades que marcarán el futuro.

Concluyó su intervención señalando que la iniciativa debe reconocer un razonable equilibrio entre tratamiento y protección de datos; definir adecuadamente el alcance que debe reunir el consentimiento para que proteja los datos de los titulares sin generar trabas en los negocios; que exista mayor claridad respecto de la permanencia de los datos a través del tiempo como una herramienta predictiva y como una manera de establecer la conducta de los titulares; mayor objetividad al momento de establecer las sanciones por parte de la Agencia de Protección de Datos, y finalmente la necesidad absoluta de incorporar el tratamiento en la ley de la información positiva.

A continuación, **el Presidente de la Comisión, Honorable Senador señor Harboe,** ofreció la palabra **al Director Ejecutivo de *Mapcity*, señor Roberto Camhi,** quien agradeció la invitación de la Comisión para exponer específicamente lo que dice relación con la localización que se genera cuando los datos están siendo utilizados por las empresas.

Consignó que *Mapcity* es una empresa que tiene más de veintitrés años en el mercado chileno y también opera en otros países de Latinoamérica. Agregó que durante estos años han venido desarrollando aplicaciones y servicios que benefician a los usuarios utilizando principalmente el dato espacial que generan las bases de datos.

Expresó que *Mapcity* ha observado cómo de manera creciente los datos han tomado cada vez más relevancia y no pueden ser excluidos de la presente iniciativa.

Indicó que los datos de geolocalización son generados de múltiples formas. Añadió que en un comienzo el dato se generaba por las propias personas, quienes entregaban una dirección y ésta luego se transformaba en una coordenada para ser puesta en un mapa. Hoy ese dato se genera de manera automática, a través de los distintos dispositivos.

Declaró que son múltiples las señales que se generan cada segundo con información proveniente de las personas y de los dispositivos que ellas utilizan. Constató que esa información es procesada a través del *Big data*, para entregar a los usuarios un mejor servicio.

Agregó que la información la entrega el usuario a cambio de un mejor servicio.

Enfatizó que *Mapcity* ha buscado segmentar a la población y al usuario de tal manera que éstos puedan ser considerados según sus intereses y así poder entregar los servicios que requieran.

Manifestó que ambos proyectos de ley promueven que no se vulneren los derechos de las personas y que no existan comunicaciones no deseadas. Indicó que la localización permite segmentar al usuario y se le entregue información relevante dependiendo de lo que él quiere y dónde se encuentra.

Destacó que el mejor ejemplo lo constituye el programa *Waze*, ya que gracias a la economía colaborativa y a la generación de la coordenada en aplicaciones permite obtener mejor información del tráfico vehicular y obtener la mejor ruta en función de la ubicación de cada una de las personas que emplean la misma aplicación.

Sostuvo que más allá de definir el listado de aplicaciones o de funcionalidades que pudiesen ser utilizadas, lo que se debe hacer es que la información se emplee correctamente y no vulnere los derechos.

Recalcó que la empresa que representa siempre ha trabajado con la información anónima, porque a partir de ella se puede generar un valor para el usuario y ella permite segmentar por grupos. Ésta solo se puede crear si se conoce la información individual. Añadió que es relevante entender bien cuando se habla de la generación del dato, puesto que si no genero el dato individual no puedo obtener el dato anonimizado.

Se preguntó cómo podemos intentar que el dato de la geolocalización, una vez que se autoriza por parte de quien lo genera, ya sea a través de una aplicación o servicio, pueda ser tratado para entregar los beneficios que las personas están esperando de dicho dato. Hizo presente que un bajo porcentaje de la población elimina el envío de sus coordenadas, porque el valor del dato geográfico le está provocando un beneficio.

Concluyó su intervención señalando que es necesario dictar una normativa que regule el mal uso de la información y que no inhiba el buen uso que se le puede otorgar a ésta.

A continuación, **el Presidente de la Comisión, Honorable Senador señor Harboe,** le ofreció la palabra **al Director Ejecutivo de la Asociación Latinoamericana de Internet (ALAI), señor Gonzalo Navarro**.

Al iniciar su intervención agradeció la invitación a esta sesión y manifestó que la Asociación Latinoamericana de Internet (ALAI) es una entidad internacional sin fines de lucro, recientemente creada, que tiene entre sus objetivos pensar y desarrollar Internet en Latinoamérica y el Caribe, representando el punto de vista del sector dedicado al desarrollo de servicios, contenidos, plataformas y aplicaciones en la región.

Agregó que parte del Directorio de ALAI son empresas como *Google, Facebook, Yahoo, Despegar, Mercado Libre, Amazon*. Aclaró que los comentarios que se viertan en la presente discusión representarán a un sector y no a las empresas mencionadas.

Recalcó que hoy en día en la cuarta revolución industrial los datos personales son la sangre por la cual fluye la economía digital.

Apuntó que un buen tratamiento de datos personales no solo permite el crecimiento económico, sino que también otorga la seguridad a los usuarios, que son la pieza fundamental y esencial de la industria de internet. Añadió que sin la confianza ni seguridad de los usuarios no existe economía digital.

Indicó que leyes que promuevan un adecuado balance respecto de la seguridad de los usuarios y que al mismo tiempo permitan generar nuevos modelos de negocios son fundamentales para la economía digital. Precisó que este equilibrio es difícil de lograr, básicamente por la velocidad en que se mueve la industria de *internet* y por la necesidad y requerimiento de los usuarios.

Señaló que la Ley Mexicana sobre protección de datos constituye un muy buen antecedente ya que incorpora las necesidades del país, con su tasa de crecimiento, con su cercanía con Estados Unidos de Norteamérica, toma lo mejor de otras jurisdicciones o bloques económicos y los incorpora a su legislación.

Estimó que lo descrito es lo que se está haciendo en las iniciativas en estudio.

En cuanto al análisis particular, advirtió que dada la importancia de las definiciones para las interpretaciones y aplicaciones de una norma de estas características, resulta fundamental simplificar para asegurar la comprensión de los conceptos.

Sostuvo que la definición de datos sensibles es excesivamente amplia y puede jugar en contra de un adecuado desarrollo de la industria y de los derechos de los usuarios. Agregó que si existe indefinición resulta difícil para las empresas establecer el ámbito de sus responsabilidades.

En cuanto a la definición para el responsable de datos, el Mensaje señala: “Responsable de datos o responsable: persona natural o jurídica, pública o privada, a quien compete decidir acerca del tratamiento de datos personales, con independencia de si los datos son tratados directamente por él o a través de un tercero o mandatario, y de su localización.”

Afirmó que la norma antes transcrita requiere de una mayor revisión. Subrayó que dicho concepto, en la práctica, convierte a cualquier sujeto de derecho en responsable, sin delimitar en forma alguna cuál es la conducta o circunstancia que le convierten en responsable, lo que acarrea una innegable indefinición y falta de certeza jurídica.

Recomendó introducir el concepto de bases de datos y definir al responsable de las mismas como aquél que decide acerca del tratamiento de las bases de datos que efectivamente obren en su poder.

Por otro lado, consideró que la referencia a la localización o ubicación del obligado resulta innecesaria y absolutamente excesiva. Se desprende de la definición en su redacción actual que cualquier sujeto que lleve a cabo cualquier tratamiento sobre cualquier dato personal estará sujeto a la futura ley chilena.

Propuso tratar por separado el tema de la jurisdicción, fuera de las definiciones y, en cualquier caso, mantener esta iniciativa alejada de alcances hiperexpansivos, que no solo resultan imposibles de aplicar sino que indudablemente acarrean problemas de

conflictos de ley imposibles de resolver, ya que el responsable que trate datos desde el exterior puede estar sujeto a otra legislación. La ley local no puede pretender ir más allá de las fronteras y pretender aplicarse a todo lo que suceda en el exterior. Lo que sí puede implementar es una exportación o circulación transfronteriza de datos segura y bajo ciertos estándares interoperables y compatibles, como ocurre en legislaciones modernas que han resultado efectivas sobre la materia, tal y como la Ley Mexicana de datos Personales.

Mencionó que dentro de la normativa general aplicable en Chile y especialmente en lo que respecta a Intermediarios en *Internet*, la figura del Intermediario fue introducida mediante la ley N° 20.435 de 2010, con el objeto de implementar las obligaciones del Tratado de Libre Comercio con Estados Unidos y por ende, la ley de Protección de Datos Personales debería seguir dicho lineamiento.

Agregó que los llamados Intermediarios de *Internet* deberían estar excluidos de la ley en relación al contenido generado por los usuarios de sus plataformas o servicios de una manera similar a la planteada en la Ley de Propiedad Intelectual.

En relación al tratamiento automatizado de datos, destacó que no solo funciona para empresas grandes a nivel global, sino que también opera positivamente para empresas locales.

Reconoció que existe una mala interpretación respecto a cómo funciona la economía digital y el tratamiento de los datos. Subrayó que cada vez surgen nuevas aplicaciones, nuevos modelos de negocios en todos los lugares del mundo. Añadió que si no permitimos que existan reglas claras y consecuentes en relación al tratamiento automatizado estaríamos poniendo obstáculos o trabas que resulten innecesarias.

Luego, manifestó que está de acuerdo en el marco de flexibilidad que se establece en el proyecto de ley en estudio al consagrar el consentimiento expreso y tácito.

Mostró su preocupación por las limitaciones que presentaría la iniciativa si mantiene el consentimiento como única forma de legitimar el tratamiento. Aseveró que en la era del *Big Data* o *Internet* de las cosas resulta imprescindible que las legislaciones se adapten a las nuevas realidades.

Agregó que siguiendo el modelo de *la Directiva Europea de Protección de Datos 95/46/CE y del Reglamento General de Protección de Datos*, los supuestos contemplados como excepciones pasarían a ser circunstancias habilitantes, en lugar de excepciones a una de las varias bases legales disponibles.

En relación con las distintas fuentes de legitimidad del tratamiento, recalcó que los intereses legítimos constituyen una base legal tan imprescindible como el consentimiento y sugirió que sea incluida en el texto final. De esta manera, el tratamiento de dichos intereses sería pionera en América Latina (países como Argentina o Brasil ya lo están considerando).

Sugirió que la ley incluya una lista no exhaustiva de supuestos que pueden considerarse como intereses legítimos. En este sentido, los considerandos números 47, 48 y 49 del Reglamento precedentemente mencionado ofrecen, entre otros, los siguientes supuestos: prevención del fraude, seguridad de redes e infraestructuras, marketing directo, administración de bases de datos de clientes y empleados.

Asimismo, aseguró que factores como la naturaleza y las características de la relación entre el titular y el responsable, o la naturaleza de la información (sensible o no), pueden resultar criterios sumamente útiles.

Destacó la necesidad de no limitar el alcance de esta base legal a ciertas categorías de datos (datos accesibles al público). Precisamente por este motivo, la legislación española que implementa la Directiva Europea de Protección de Datos se vio invalidada de forma parcial tras una sentencia de la Corte Europea de Justicia de 2011. En este caso, el tribunal interpretó que la norma española, que limitaba el uso de esta base legal a las bases de datos de carácter público, estaba contraviniendo la Directiva, y obligó a la reforma de la ley.

Reseñó que la Asociación que representa fue recientemente creada, sin embargo han opinado en cuatro procesos de reforma de datos personales en la región, a saber, Panamá, Ecuador, Colombia y Argentina. Agregó que actualmente en Colombia existe una interpretación de una persona, la Directora de Datos Personales respecto de puntos de ley que obedecen a un solo criterio y que no puede ser contrastado con otros dentro de la discusión sobre temas importantes como la calificación de países adecuados y no adecuados respecto de la protección de datos personales. Al no existir un organismo colegiado se corre el riesgo de que el debate se centre en una sola mirada.

Seguidamente, **el Presidente de la Comisión, Honorable Senador señor Harboe,** ofreció la palabra a **la Directora Ejecutiva de la Fundación Datos Protegidos, señora Romina Garrido**.

La señora Garrido comenzó intervención agradeciendo la invitación que se les hizo llegar para exponer puntos de vista de la sociedad civil interesada en la protección los datos personales. Señaló

que la ONG Datos Protegidos es una organización privada preocupada del empoderamiento de las personas en el mencionado derecho, indispensable en la era digital, pero también en los entornos físicos. Agregó que asimismo se ocupan de la defensa y del ejercicio de la ley N° 19.628, a través de las acciones judiciales.

Manifestó que el proyecto de ley del Ejecutivo, en su artículo 30, crea la Agencia de Protección de Datos Personales. Afirmó que la eficacia de cualquier legislación de protección de datos personales radica en su autoridad de control. Asimismo, explicó que la ley N° 19.628 padece de un desequilibrio en cuanto a los derechos de las personas.

Sostuvo que estamos en una oportunidad histórica de poder equilibrar esta balanza, que ha estado cargada durante todo este período para el tratamiento de los datos como un capital de negocios y no como derechos ciudadanos.

Luego, expresó que la independencia de la autoridad de control determinará su eficacia. Añadió que no solo es necesaria una independencia técnica. Recalcó que lo que se necesita otorgar a una autoridad de control en materia de datos personales es estabilidad, dadas las presiones que provienen desde el mercado y también desde el tratamiento de datos del Gobierno.

Aseveró que la mencionada estabilidad no está dada en la iniciativa del Ejecutivo, puesto que se somete a un nombramiento bajo el sistema de alta dirección pública, procedimiento que ha tenido fallas durante su ejercicio y que ha sido modificado recientemente.

Connotó que el sistema antes mencionado es bastante frágil y que coincide en que los años en que hay cambio de gobierno renuncian casi todas las autoridades que han sido nombradas mediante dicho mecanismo. Detalló que el año 2010 hubo 104 renuncias y en el 2014, 255 renuncias no voluntarias.

Advirtió que si bien el procedimiento está siendo corregido, la ONG que representa propone que se busque un sistema de estabilidad similar al nombramiento del Fiscal Nacional Económico. Recordó que éste es designado por el Presidente de la República bajo el sistema de Alta Dirección Pública y solo puede ser removido y sancionado, según proponga la Contraloría General de la República, previo sumario instruido por ésta; ejerce su cargo por cuatro años, y puede ser renovado por una sola vez.

En relación al nombramiento, esta autoridad no puede responder a consideraciones político partidistas. Ella debe ser independiente. Añadió que debe tener un mandato y duración definida. Debe

ser inamovible en el tiempo, para asegurar su independencia. Las causales de remoción deben estar previamente definidas en la ley.

Asimismo, hizo presente que la independencia funcional también es importante. Agregó que la Agencia debe ser independiente del poder político imperante y se debe expresar en el ámbito orgánico y material.

Sostuvo que la autoridad de control que se propone está sujeta al Ministerio de Hacienda. Recordó que conoce un caso similar en Nicaragua y aún la autoridad no puede ejercer sus funciones puesto que no se ha dictado el Reglamento que la habilitaría para comenzar a actuar. Añadió que la Agencia debiese contar con las facultades con las que cuentan los otros organismos que pertenecen al mencionado Ministerio, como la Unidad de Análisis Financiero.

Admitió que como está regulada la Agencia, estamos en presencia de una autoridad débil, donde las facultades fiscalizadoras no son claras.

Respecto al tratamiento de datos personales por organismos públicos, manifestó que se debe mejorar el régimen de licitud del mencionado tratamiento, sujetando a tales entidades a ciertas normas y no todo al estatuto de control.

Expuso que el proyecto de ley señala que los organismos públicos quedan exentos del régimen fiscalizador y sancionatorio de la Agencia de Protección Datos Personales. Recalcó que las personas que se sientan afectadas por un tratamiento de datos por el sector público, tendrán que acudir a la Corte de Apelaciones respectiva.

Lo anterior, continuó, muestra que estamos ante una Agencia que no está al nivel de los otros organismos públicos y desincentiva a que las personas puedan denunciar malas prácticas que provengan de los mencionados organismos. Enfatizó que el proyecto debe ser corregido en ese sentido.

Precisó que se excluye del régimen de tratamiento de datos de organismos públicos todos aquellos relativos a seguridad pública.

Afirmó que la fuente de acceso público debe ser cerrada, para evitar los abusos que actualmente existen respecto de los datos personales que circulan por internet. Agregó que el concepto de dato sensible debe ser abierto, porque busca proteger a las personas.

En relación a la figura de los intermediarios incorporada en la Moción, estimó que ella debe ser mantenida. Afirmó que éstos deben ser igualados a los encargados.

Finalizó su intervención señalando que la extraterritorialidad de la ley y la designación de un responsable en Chile constituyen un avance para los derechos ciudadanos. Agregó que hoy en día las personas no tienen dónde recurrir cuando tienen un problema con tratamiento de datos que se realizan en otros países cuando no hay representantes en Chile.

A continuación, **el Presidente de la Comisión, Honorable Senador señor Harboe**, ofreció la palabra **al Director de Hermann Consultores, señor Jorge Hermann.**

El señor Hermann manifestó que asiste en calidad de profesor de la Escuela de Negocios de la Universidad de Chile. Señaló que fue Jefe de Estudios del Ministerio de Economía y le correspondió participar en la elaboración del proyecto de ley que presentó el Gobierno anterior, sobre datos personales.

Expresó que la protección de los datos personales y la seguridad informática pueden ser temas complejos de entender para una persona común y corriente, pero es algo que afecta la vida cotidiana de la mayoría de la población que utiliza internet. Por lo cual, es importante fomentar una regulación adecuada al respecto.

Indicó que en la era digital, la obtención y el almacenamiento de la información personal son esenciales. Los datos son utilizados por todo tipo de empresas tales como instituciones financieras, retail, redes sociales y motores de búsqueda.

Declaró que en un entorno globalizado, la transferencia de información entre países es algo cotidiano. En internet no hay fronteras y el uso del cloud computing permite que los datos se envíen entre continentes en un par de segundos.

Hizo presente que las empresas tienen mucha más información de sus clientes. Apuntó que las redes sociales y motores de búsqueda están produciendo cada vez más información personal, que está a disposición de las empresas que quieren enviar publicidad a sus clientes de manera particular y oportuna.

En seguida, añadió que al mismo tiempo, los hackers son cada vez más astutos en el robo de los datos personales almacenados en las empresas, por lo que asegurar la enorme cantidad de información es cada vez más complicado.

Recordó que, actualmente, el uso del *cloud computing, smartphones y tablets* adiciona un desafío extra para salvaguardar la información personal.

Por lo anterior, los gobiernos están cada vez más preocupados por la privacidad de los datos de las personas en todo el mundo y el gobierno de Chile está atrasado en la materia, según el informe *Digital Economy 2015* de la OCDE.

A continuación, recalcó que es urgente una reforma que garantice a las personas naturales el legítimo ejercicio de su derecho a la protección de su vida privada y un tratamiento correcto de sus datos personales bajo estándares internacionales. Llamó la atención de que Chile y Turquía son los únicos países dentro de la OCDE que no han realizado ningún avance en mejorar la protección de la información, lo cual es grave y preocupante.

Aseveró que en el gobierno del ex presidente Piñera se ingresó un proyecto de ley que mejoraba la actual legislación del año 1999, la cual fue desechada por el actual gobierno, quien ingresó un proyecto de ley similar con una agencia de datos personales análoga a la europea.

Connotó que la OCDE ha señalado que Chile está incumpliendo el acuerdo sobre mejorar la legislación de datos personales, que fue establecido cuando nuestro país ingresó a este grupo de economías avanzadas en el 2010. Prueba de ello, es la carta de advertencia que envió la OCDE al Ministerio de Economía en julio del 2015 sobre el lento avance que ha tenido la legislación para perfeccionar la protección de datos personales.

Por otra parte, consignó que el Ministerio de Hacienda está a cargo del proyecto de ley que mejora tres artículos que componen el título III sobre Información y Consolidación de Deuda Crediticia de la Ley de Datos Personales a través de un registro único sobre deudas morosas (negativas) y al día (positivas) que las personas tengan en bancos, *retail*, cooperativas, cajas de compensación, entre otras, cuya operación debe ser consensuada entre los actores crediticios y la autoridad.

Destacó que es recomendable aprobar con rapidez el proyecto de ley sobre datos personales en el Congreso. Lo ideal sería tramitar en conjunto datos personales e información crediticia. Pero, dado que somos el único país de la OCDE que no ha hecho nada al respecto, es preferible avanzar primero en datos personales por sus amplias implicancias en todos los sectores de la economía y luego continuar con información comercial que es más difícil de resolver legislativamente.

Por lo tanto, un marco más sólido y claro de protección de datos incentivará a las personas y empresas a sacar el máximo provecho del mercado digital, fomentando el desarrollo económico, la innovación y la productividad en nuestro país.

Seguidamente, aseveró que los proyectos de ley en discusión resultan interesantes, y vienen a modernizar una legislación que no está actualizada.

Agregó que tanto el Mensaje como la Moción incorporan principios reconocidos por la OCDE. Asimismo establecen el "consentimiento del titular" con el objeto de enmarcar que la licitud de todo tratamiento de datos personales requiere la manifestación expresa de voluntad de su titular a través de declaración verbal, escrita o medios electrónicos.

Manifestó que ambas iniciativas vienen a reforzar el derecho a la información a los titulares de datos personales y las obligaciones del responsable del tratamiento de éste. También hacen hincapié en la protección especial para niños y adolescentes. Asimismo, hizo presente que ambos cuerpos legales regulan el flujo transfronterizo de datos.

Recalcó que el proyecto del Ejecutivo crea una Agencia de Protección de Datos Personales que dicta instrucciones y normas generales, interpreta la ley, fiscaliza y multa. Asimismo incentiva la autorregulación con certificación y programa de cumplimiento voluntario.

Remarcó que no obstante lo anterior, existen algunos aspectos que deben ser mejorados para perfeccionar y robustecer el proyecto de ley. Entre ellos destacan los siguientes:

i) Una institucionalidad más moderna

Indicó que la Agencia de Protección de Datos Personales es un organismo público, encargado de velar por el cumplimiento de la ley y dependiente del Ministerio de Hacienda, a cargo de un director elegido por Alta Dirección Pública. La Agencia fiscaliza, interpreta administrativamente las disposiciones legales, dicta normas generales e imparte instrucciones y multa.

Sugirió que la mencionada Agencia sea una corporación autónoma de derecho público, con personalidad jurídica y patrimonio propio, independiente, que conste de un gobierno corporativo compuesto por un consejo independiente de cinco miembros elegidos por el Presidente de la República, ratificados por el Senado, que será responsable de la dirección técnica sobre fiscalizar, normar, interpretar y multar. También,

que el consejo proponga un director ejecutivo que estará a cargo de la administración y ejecución de las directrices técnicas de la institución.

Asimismo, planteó la necesidad de eliminar las funciones de dictar instrucciones y normas generales. Se debe, señaló, incorporar la posibilidad de proponer recomendaciones normativas al Gobierno, para modificar la ley o reglamentos que regulan esta materia.

Igualmente, se mostró partidario de suprimir las atribuciones de multar. Este organismo debe ayudar a los consumidores a preparar la prueba y los antecedentes necesarios para demandar a la empresa infractora en los tribunales de justicia.

Indicó que en caso de que se insista en mantener la estructura de la Agencia, ésta debería depender del Ministerio de Economía porque todas las materias relacionadas con el consumidor (Sernac y FNE) están bajo su alero y permite una mejor coordinación sistémica.

ii) Pymes

En seguida , hizo presente que el proyecto de ley establece una carga regulatoria importante de trabajo y recursos a las empresas para un aplicación correcta de la protección de los datos personales, tales como hacer frente a los derechos de los titulares (acceso, rectificación, cancelación, oposición, portabilidad) y obligaciones del responsable de datos (art. 14 bis, ter y quater).

Sugirió que esta iniciativa consagre la diferenciación de estándares de cumplimiento para las Pymes por medio de la dictación de un reglamento. No obstante, es necesario que quede establecido claramente en la ley cuáles materias deben ser cumplidas por las Pymes.

Añadió que en las multas se establece el criterio del tamaño de las ventas para determinar el monto de las mismas, pero nada se dice sobre considerar un tratamiento especial para las pymes a través de un esquema de sustitución de multas por capacitación con una regulación más orientadora y menos punitiva como sucede en el estatuto pyme. Propuso establecer un modelo de prevención de infracciones, más simple y menos engorroso para estas pequeñas empresas.

Por último, consignó que la aplicación de la ley sea primero en las grandes empresas y después en las pymes, para tener un periodo de prueba de la nueva legislación.

iii) Tratamiento desigual al sector privado versus el sector público

En este ámbito, manifestó que para un mismo tipo de dato personal se requiere consentimiento del titular en su tratamiento por parte de la empresa privada, y no así en el caso de los organismos públicos. Pero, se establece que al momento de comunicar o ceder los datos personales por una institución pública se necesita del consentimiento del titular previamente.

Sostuvo que en el régimen de excepciones de aplicación de la ley por normas de secreto o confidencialidad a los órganos públicos, es recomendable dejar explícito que están excluidos el Banco Central, Instituto Nacional de Estadísticas y Servicio de Impuestos Internos.

En relación a las infracciones y sanciones a funcionarios públicos, destacó que se establece multa de 20% a 50% de la remuneración mensual de la autoridad del órgano público y no se indica la sanción de destitución para casos de infracciones gravísimas. En el caso del funcionario infractor es en cierto grado similar. Precisó que es recomendable no aplicar una estructura sancionatoria especial para datos personales y propuso ceñirse directamente a las disposiciones que sobre la materia establece la ley Nº 18.834 sobre Estatuto Administrativo.

iv) otros

En un apartado final de su exposición se refirió a los siguientes temas:

1) Explicó que en el tratamiento de los datos personales sensibles se requiere el consentimiento del titular salvo cuando el tratamiento es realizado por una fundación, una asociación o institución sin fines de lucro (política, filosófica, religiosa cultural, deportiva etc.).

Resaltó que no hay razón alguna para diferenciar entre empresas con fines de lucro y sin fines de lucro. Recomendó que exista consentimiento en ambos casos, en especial cuando el dato sensible está relacionado a la identidad genética y biomédica (salud).

2) En el tratamiento de datos personales para fines históricos, estadísticos, estudios e investigaciones se requiere consentimiento del titular para su tratamiento y medidas de seguridad.

Propuso incorporar, al final del artículo, la idea de que los datos utilizados para los fines establecidos en la ley, se podrán tratar sin limitaciones cuando previamente hayan sido anonimizados.

3) En la transferencia internacional de datos personales se establece que la Agencia determinará los países que poseen adecuados estándares de protección de datos.

Sugirió establecer un plazo claro para que la Agencia se pronuncie al respecto.

4) Se mostró partidario de incorporar que el gobierno presente una evaluación de impacto regulatorio de la institucionalidad de protección de datos personales a los 2 y 4 años de la aplicación de la ley.

Finalmente señaló que es recomendable crear un grupo consultivo sobre datos personales para que participe el sector privado y público con comentarios, sugerencias y modificaciones para mejorar la institucionalidad de datos personales.

A continuación, **el Presidente de la Comisión, Honorable Senador señor Harboe,** ofreció la palabra **al Presidente de la Fundación Pro Acceso, señor Juan Pablo Olmedo**.

El señor Olmedo agradeció la invitación de la Comisión a exponer sobre esta iniciativa. Hizo presente que junto con ser el Presidente de la Fundación antes mencionada, asesora en materias legislativas al Honorable Senador señor Larraín.

Manifestó que la iniciativa de Su Excelencia, la Presidenta de la República, señora Michelle Bachellet de crear una Agencia de Protección de Datos Personales que se contiene en el Boletín N° 11.144-07, resulta oportuna y es bienvenida. Agregó que correspondía felicitar la disposición del Ministerio de Hacienda para asumir el liderazgo de fortalecer la institucionalidad de protección de datos personales en Chile. Añadió que similares iniciativas de reforma impulsadas en los dos gobiernos anteriores -emanadas de la Secretaria General de la Presidencia y del Ministerio de Economía-, no lograron concitar los apoyos institucionales y generar consenso al interior de la propia Administración y en el Congreso Nacional.

En seguida, se refirió en particular a las siguientes materias que considera el proyecto en análisis:

1.- Autonomía Legal

Expuso que en el escenario institucional de Chile la creación de autonomías legales tienen un rol coadyuvante de la Administración y cuentan con facultades de fiscalización y de garante de derechos fundamentales. Tal es el caso, explicó, del Consejo para la Transparencia, del Consejo del Servel y del Instituto Nacional de Derechos

Humanos. Indicó que una de las razones que explican la creación de las autonomías legales fue la contribución de una sociedad civil persistente y resuelta que fue capaz de revertir y doblegar la tendencia centralista de la Administración. Y para ello se acudió a novedosas herramientas de control social que, para el caso de la ley Nº 20.285 Sobre Acceso a la Información Pública, incluyó una sentencia de la Corte Interamericana de Derechos Humanos.

Agregó que la experiencia acumulada en el desarrollo e inserción de esta estructura jurídico-institucional de autonomía legal tiene de dulce y agraz. Siendo un triunfo para sentidas reivindicaciones de empoderamiento social, en una cultura administrativa de marcado arraigo presidencial como la chilena tal modalidad resulta excepcional, es vista como una anomalía institucional, y presenta enormes desafíos y obstáculos en su desarrollo.

Sostuvo que la Agencia de Protección de Datos Personales responde a una exigencia de inserción internacional de Chile en el marco de los compromisos de la OCDE. Su objetivo mayor es el regular los flujos de intercambio internacional de datos para ser considerado país seguro. Agregó que al no proceder la exigencia de adecuación institucional de una sentida demanda ciudadana, la decisión del Poder Ejecutivo de optar por la creación de una Agencia de Protección de Datos Personales bajo la tuición del Ministerio de Hacienda no resulta extraña.

Seguidamente, consignó que la misma, de ser ratificada, genera un alejamiento de la irradiación de la competencia autónoma del Consejo para la Transparencia. Las atribuciones conferidas en el proyecto de ley del Ejecutivo a la Agencia de Protección de Datos en el artículo 31) para vincularse con los otros poderes del Estado y de interlocución y cooperación internacional y, la modificación al artículo 33 letra m) de la ley Nº 20.285 -que establece el artículo 2 transitorio del proyecto de ley- que limita su actuación de protección de datos a los ámbitos de transparencia de la función pública y el acceso a la información, conlleva una derogación de las competencias asignadas a la autonomía legal en el artículo 33 m de la Ley Nº 20.285. A ello, se suma la ausencia de instancias para la solución de conflictos entre la Agencia y el Consejo para la Transparencia, obligando a una solución externa que no es otra que judicialización entre órganos del Estado, lo que no es un sano criterio de política pública.

2-. Autonomía Funcional.

En esta ámbito apuntó que cabe preguntarse por la consagración de una autonomía funcional, es decir, que no obstante su dependencia jerárquica al Gobierno Central incorpore elementos que la

hagan apta para asegurar la protección y deferencia al derecho fundamental a la protección de los datos personales, otorgue un tratamiento igualitario al sector público y privado, dé certeza país al tráfico internacional de datos; se inserte y colabore de manera armónica al interior del Estado; y, sea reconocida y validada por la ciudadanía.

Hizo las siguientes observaciones para el caso que la decisión estatal sea mantener las competencias de tuición de los datos personales al interior de la Administración:

a. La práctica comparada delega tal función en órganos con mayor cercanía y sensibilidad con la temática, como son el Ministerio de Economía o el Ministerio de Justicia. La propuesta de radicar en el Ministerio de Hacienda tal función a través de la Agencia merece ser analizada con especial atención. Más allá del prestigio institucional, las competencias de generación de política pública y protección de derecho fundamentales son ajenas al mandato institucional del Ministerio de Hacienda que lo orienta a la dirección de la política financiera, de recaudación de rentas públicas, de contabilidad general, entre otras, pero no a la protección del derecho a la protección de datos personales. (DFL Nº 7.912).

Puntualizó que la dependencia orgánica y jerárquica de la Agencia de Protección de Datos del Ministerio de Hacienda se constata, por ejemplo, en los artículos 30, 31, 32 y 33 del proyecto.

b. La unidad técnica (Agencia de Protección de Datos) muestra en su actual propuesta obstáculos a la protección de los derechos fundamentales de los chilenos. El proyecto establece un procedimiento diferenciado de reclamo frente a infracciones al derecho fundamental a la protección de datos personales, expresada, entre otras, en la diferenciación para el ejercicio de los derechos ARCO entre el sector público y el sector privado. Tal diferenciación resulta arbitraria y debe ser analizada en función del artículo 43 y siguientes de la Declaración que consagra el derecho a presentar su reclamación ante la autoridad de control, así como recurrir a la tutela judicial para hacer efectivos sus derechos conforme a la legislación nacional del Estado Iberoamericano que resulte aplicable en la materia.

c. Limitadas facultades para fiscalizar y sancionar a los organismos del Estado que por lejos son el mayor tratador de datos personales en Chile (artículo 33 g y h). Agregó que debe ser corregida en función del artículo 42.4 de la Declaración que no hace tal distinción y, por el contrario, dispone que se deberá otorgar a las autoridades de control suficientes poderes de investigación, supervisión, resolución, promoción, sanción.

d. El régimen de excepciones del proyecto de ley lo identifica con “órganos públicos” que tratan datos en materias de investigación y sanción penal, civil o administrativa, lo que excluye a un significativo grupo de organismos, como Carabineros, PDI, tribunales, Ministerio Público, etc., muchos de ellos tratadores de datos sensibles y de especial preocupación ciudadana. Tal definición debe ser precisada con mayor detalle otorgando garantías adecuadas para evitar accesos o transferencias ilícitas o desproporcionadas, la determinación del responsable o responsables, entre otras.

e. La transferencia internacional de datos que autoriza los artículos 27 y siguientes de la iniciativa del Ejecutivo debe ser revisada y complementada para fortalecer las instancias de transparencia y rendición de cuenta de tal función, autorizar y validar cláusulas contractuales o instrumentos jurídicos que faciliten el intercambio y cooperación y establecer límites a las transferencias internacionales de categorías de datos personales por razones de seguridad nacional, seguridad pública, protección de la salud pública, protección de los derechos y libertades de terceros, así como por cuestiones de interés público.

Manifestó que considerando las insuficiencias de autonomía funcional de la Agencia y ante la negativa del Estado de creación de una autonomía legal como responsable de la tuición del derecho a la protección de los datos personales, se requieren significativas mejoras institucionales.

Valoró la iniciativa del Ministerio de Hacienda en la propuesta de la Comisión de Valores cuyo gobierno corporativo recae en manos de una autoridad unipersonal de confianza del Presidente de la República y un de Consejo de 5 miembros. De esta manera, el fortalecimiento de la Agencia en el sentido señalado por el propio Ministerio de Hacienda, sería una positiva señal.

Concluyó su intervención señalando que atendida las particularidades y desafíos propios de esta reforma, el llamado a ser parte del Consejo de la Agencia de Protección de Datos Personales podría incorporar al Consejo para la Transparencia, al Ministerio de Economía y al Ministerio de Justicia, y fortalecer a referentes sociales expertos de la sociedad civil, el sector privado y el mundo académico. Así también se satisface el desarrollo orgánico de la Administración, se recoge la experiencia acumulada por parte del Consejo para la Transparencia y el Ministerio de Economía y se favorece la legitimación social.

A continuación, **el Presidente de la Comisión, Honorable Senador señor Harboe,** ofreció la palabra **al Director del Centro de Estudios de Derecho Informático de la Universidad de Chile, señor Renato Jijena.**

El señor Jijena comenzó su presentación señalando que estamos en presencia de un debate sin una definición previa de política pública.

Se preguntó qué nos convoca en la presente discusión. Manifestó que estamos hablando de datos personales o nominativos, definidos en el artículo 2° de la ley N° 19.628 que señala: “f) datos de carácter personal o datos personales, los relativos a cualquier información concerniente a personas naturales, identificadas o identificables”. Agregó que es partidario que este tema se extienda a las personas jurídicas, a las empresas, tal como sucede en la legislación comparada.

Expresó que el nombre y los apellidos están dentro de la esfera pública. Acotó que por ley, la cédula nacional de identidad es un dato público. Agregó que en materia de sistemas, la mencionada cédula es un indexador, que permite asociar, otros antecedentes personales.

Expuso que en cuanto a la edad y el domicilio, son datos que figuran en fuentes públicas en distintas instancias y nadie podría entender que con esa información se está vulnerando la privacidad o se está atentando en contra de sus datos personales, o con el derecho de acceso a la protección de datos.

Respecto al credo religioso, señaló que éste constituye un dato sensible y personalísimo que debe tener un resguardo especial.

Luego, indicó que surgen complicaciones cuando hablamos de la etnia, la opción sexual y la filiación política. Recordó que esta última, de acuerdo a nuestra Carta Fundamental es un dato secreto o reservado.

Consignó que el Consejo para la Transparencia, alejado de la sensibilidad con la protección de datos, autorizó a pedir toda la información de los discapacitados en Chile y obligó al Servel a entregarla, porque era generada con fuentes públicas.

Apuntó que se debe regular el tema de los datos biométricos (huella digital), que se usa como un autenticador en el comercio. Agregó que el Consejo para la Transparencia quería obligar al Servicio de Impuestos Internos, saltándose el secreto tributario, a entregar toda la base de datos de los contribuyentes de bienes raíces de la región de Arica, por la misma razón esgrimida en la anterior solicitud. Connotó que fue la Corte de Apelaciones la que impidió la entrega de dicha información.

Recalcó que la información sobre las deudas ya está regulada en Chile y es importante que se conozca. Asimismo, hizo presente que las líneas aéreas, las agencias de turismo y los hoteles, están intercambiando los hábitos preferenciales de los comportamientos de los ciudadanos en materia de viaje, ya sea dentro o fuera de Chile.

Manifestó que los datos del sector público operan dentro del marco de su competencia, tienen atribuciones legales, responsabilidades administrativas establecidas en la ley y son fiscalizados por la Contraloría General de la República.

Asimismo, sostuvo que en el sector privado el tratamiento de datos personales genera una materia prima relevante de la gestión de importantes empresas (bancos, tiendas de *retail*, compañías de seguros, Isapres, AFP, etc.). Agregó que es acá donde se produce un negocio de transferencia de bases de datos que regular en forma idónea, que hoy se desarrolla en una zona oscura, que factura millones (*list brockers*). Enfatizó que esto último constituye una omisión de importancia en el proyecto de ley del Ejecutivo, no así de la Moción.

Recalcó que una mala regulación significa una desregulación y es ahí donde cobra importancia el registro, las sanciones, la fiscalización y la relación entre un órgano garante y que defiende los derechos de los titulares con las empresas privadas que están dentro del negocio.

Seguidamente, hizo presente que las leyes de protección de datos personales poseen cuatro partes esenciales, a saber: dogmática; orgánica; procedimental y sancionatoria. Reconoció que, en ese sentido, ambos proyectos apuntan a subsanar los defectos de la legislación vigente.

Agregó que en la parte dogmática se consagra el llamado "*habeas data*" o derecho de acceso, que es radicalmente distinto al derecho de acceso a la información.

Señaló que en cuanto a la parte orgánica se crea una autoridad de control que administra un registro obligatorio de bases de datos y aplica sanciones administrativas. Sostuvo que comparte las finalidades que se le otorgan a la Agencia de Protección de Datos.

Manifestó que la iniciativa del Ejecutivo, desde el punto de vista del proceso, contempla un procedimiento contencioso administrativo para que los titulares hagan valer su "derecho de acceso" de manera sumaria y breve. Respecto a la parte sancionatoria, destacó que se establecen sanciones civiles, multas e incluso sanciones penales.

Connotó que la ley N° 19.628, sobre protección de la vida privada, posee una parte dogmática débil, no tiene parte orgánica real, no contempla procedimientos administrativos de tutela sino uno judicial, y no posee un arsenal sancionador adecuado.

Atendido este escenario, resaltó que en Chile se usan los datos con diversos fines, no apegados a los declarados al ser recopilados. Abogó por una fiscalización administrativa del uso de datos realmente conforme a los fines declarados.

Añadió que en el artículo 4° de la ley N° 19.628 se exige consentimiento previo y expreso del titular para el tratamiento de datos, pero tiene tal cantidad de excepciones que en la práctica se puede procesar datos sin autorización. Aseveró que el proyecto de ley del Ejecutivo propone consentimiento tácito. Solicitó que este tema sea debatido en profundidad.

Reseñó que en Chile, los responsables de bases de datos son anónimos, porque no están registrados ante una Autoridad de Control que administre el registro. Afirmó que la iniciativa del Ejecutivo lo suprime por costos administrativos, supuestamente siguiendo el criterio de la Unión Europea. Observó que nuestro país no tiene cuarenta años de institucionalidad y esto mantiene la impunidad del tráfico de bases de datos con fines de lucro.

Luego, aseveró que ambas iniciativas buscan optimizar los aspectos dogmáticos, y los dos mejoran sustancialmente el estado del arte. Se mostró de acuerdo en que el proyecto de ley del Ejecutivo contemple la existencia de un órgano competente. Indicó que la mencionada iniciativa propone reemplazar el procedimiento judicial por un contencioso administrativo.

Observó que ambos proyectos le conceden la importancia debida a la seguridad de sistemas y ambos explicitan las posibles sanciones o multas pecuniarias. Reconoció que éstas son elevadas -para las pymes-, sin parámetros de cálculo y con el error de llegar a impedirse el funcionamiento vía sanciones accesorias. Destacó que faltan elementos de cálculo y parámetros concretos para llegar a establecer la multa. Enfatizó que la autoridad de control no se puede financiar a través de las multas.

Manifestó que el rol de la Agencia de Protección de Datos es preventivo, educativo, es de establecer parámetros mínimos y sociabilizar, tal como lo ha hecho el Consejo para la Transparencia.

En seguida, añadió que ambos proyectos de ley buscan acercarse a estándares de la Unión Europea, ambos aumentan los deberes, las cargas, las responsabilidades y las sanciones para los

responsables de las bases de datos, y mejoran sustancialmente los derechos para los titulares y propietarios de la información nominativa. Advirtió que desconoce si Chile, en esta primera etapa, requiere estándares tan altos de regulación.

Apuntó que los roles fiscalizadores, reguladores y promocionales asignados al órgano de control unipersonal propuesto son idóneos, y los grados de descentralización funcional que el derecho chileno le asignaría también son adecuados para una primera etapa de instalación y posicionamiento.

Advirtió que la regla general son las autoridades unipersonales y el único caso donde deficitaria y erradamente se mezcla este tema con el ámbito de la probidad y la transparencia se produce en México.

Finalmente, hizo referencia a un informe del Centro de Sistemas Públicos de la Escuela de Ingeniería Industrial de la Universidad de Chile, del año 2010, que diseñaba un modelo organizacional del Consejo para la Transparencia en su función de protección de datos personales. En él se señala: “Un aspecto crítico que hace dudar de la conveniencia de que ambas funciones (Protección de Datos y Acceso a la Información) estén en una misma institución es que el "negocio" de la Protección de Datos es muy distinto al del Acceso a la Información.

Esto se puede ver descrito en una serie de factores como:

a. Principios: Ambos principios (Acceso a la Información y Protección de Datos) tienen orígenes y focos muy distintos e incluso contradictorios.

b. Funciones: El negocio de la Protección de Datos está orientado hacia la seguridad y tratamiento de información con procesos de alta complejidad. Tanto los procesos como los perfiles profesionales que se requieren son muy distintos a lo que puede ser en Acceso a la Información donde el foco está hacia la adopción de buenas prácticas en el sector público y no hacia la fiscalización de procesos complejos.

c. Mercados: El mercado principal de la Protección de Datos está en el sector privado. Es en este sector donde se encontrarán los principales detractores del Consejo en su función, donde se tendrá que lidiar con industrias enteras dedicadas a lucrar con la información personal de terceros y donde se presentarán los mayores desafíos a la regulación. El mercado del Acceso a la Información es el sector público y, los dilemas entre ambas están orientados a la primacía de un derecho sobre el otro y la construcción de dicha normativa.

d. Conflictos de intereses: La institucionalidad ligada al Acceso a la Información está pensada principalmente en su independencia frente al Poder Ejecutivo. En el caso de la Protección de Datos los principales conflictos de intereses se darán con el sector privado, por ende se torna mucho más complejo.”

Finalizó su intervención señalando que la Agencia debe enfocarse en el sector privado, que es el ámbito donde más se utiliza información y el envío de datos constituye un gran negocio.

A continuación, **el Presidente de la Comisión, Honorable Senador señor Harboe**, ofreció la palabra **a la Directora Ejecutiva de la ONG Derechos Digitales, señora María Paz Canales.**

La señora Canales comenzó señalando que es una preocupación de la ONG que representa la asimetría que se establece entre la posibilidad de ejercer derechos por parte de los titulares de datos en relación a los organismos públicos versus las entidades privadas.

Estimó que el procedimiento que instituye una vía contencioso administrativa para poder ejercer las garantías de la normativa, que se contempla en relación al uso o mal uso de los datos personales por parte de entidades privadas, genera un obstáculo y una diferencia que carece de sentido en el mundo de hoy para el ejercicio de los derechos fundamentales de las personas en relación a la utilización de sus datos.

Observó que lo anterior es perjudicial y no se atiene a los estándares internacionales, porque el Estado es uno de los principales titulares de información de datos personales de la ciudadanía en general, y por lo tanto, la posibilidad de que ellos sean utilizados de manera arbitraria por parte de organismos públicos es equivalente a la del riesgo que existe de que eso suceda por el mundo privado. Agregó que entienden que debiera existir un mecanismo que sea equivalente para ejercer esos derechos en cualquiera de ambos casos.

Relató que lo anterior se ve agravado, porque en el caso particular de la regulación que se contempla, no están todos los derechos Arco garantizados respecto de los organismos públicos. Detalló que están los derechos de acceso y de rectificación, pero no los de eliminación y otros derechos de portabilidad. Reconoció que lo anterior no corresponde a los estándares internacionales.

Manifestó que se puede entender en un principio la distinción que se quiso hacer, de sacar a los organismos públicos de la posibilidad que la Agencia de Protección de Datos sea la encargada de juzgar si el comportamiento de otros organismos públicos corresponde o no

respecto al procesamiento de datos personales. Lo anterior se resuelve con la creación de una Agencia fuerte e independiente. Será ella la que tendrá la experiencia y podrá ir sentando criterios.

Luego, recalcó que lo anteriormente planteado es algo que se puede corregir durante el curso de tramitación de este proyecto de ley.

Reconoció como un retroceso la ausencia de la exigencia de un Registro Nacional de Datos Personales en la iniciativa. Sostuvo que el mencionado registro desempeña una función relevante en transmitir una señal que alinee los incentivos económicos para que las empresas el día de mañana decidan ajustar su comportamiento a la normativa que en definitiva se apruebe.

Consignó que si no existe el mencionado reglamento disminuyen los incentivos para ponerse al día con rapidez a los estándares que se están tratando de mejorar a través de este proyecto.

Asimismo, señaló que en relación a la definición de datos personales, se mantiene la ambigüedad actual, agregando el requisito de que la vinculación a una persona natural identificada o identificable se realice a través de “medios razonablemente utilizados”. Añadió que esta cualificación puede ser peligrosa porque ha sido cuestionada en diversas situaciones la posibilidad de asociar diferentes bases de datos para poder determinar la identificación de una persona. Destacó que al agregar la cualificación de medios razonablemente utilizados se mantiene la ambigüedad respecto de varios casos en que el ejercicio de poder identificar a una persona es relativamente fácil cuando una misma entidad tiene información de diferentes fuentes y ésta puede ser cruzada.

Constató que la disposición debiera avanzar en la línea que contempla el Reglamento de la Unión Europea en donde se refiere a medios directos o indirectos de identificación y da ejemplos que facilitan la interpretación de la disposición.

En cuanto a los datos sensibles, remarcó que se eliminan de la definición los hechos o circunstancias de la vida privada, entre ellos los “hábitos personales”. Esto deja la puerta abierta a la recolección de hábitos de consumo, por lo mismo, se sugiere su reincorporación. Del mismo modo, no se requiere consentimiento para datos personales que su titular “ha hecho manifiestamente públicos”, alejándose de la tendencia internacional de implementar el principio de contexto. Se sugiere la eliminación de dicha causal.

Respecto a la fuente accesible al público, expresó que se contempla una imprecisión en la normativa establecida en el proyecto

de ley del Ejecutivo, puesto que deja abierta la posibilidad de que la puesta a disposición de la base de datos no satisfaga los requerimientos de consentimiento y finalidad, pero que el acceso a usuarios no pueda ser calificado como ilícito en sí mismo. Esta imprecisión requiere ser subsanada para no generar un resquicio legal que permita considerar como fuentes accesibles al público bases de datos que generen perjuicio para los titulares.

En relación a la anonimización, explicó que el proyecto permite considerar como anónimo un dato susceptible de re-asociarse en la medida que no se requiera un “esfuerzo no razonable” para ello. Esto permitiría calificar como datos anónimos aquellos que no son los realmente, pues se puede revertir su anonimización.

En cuanto al consentimiento tácito, destacó que la norma que propone el Mensaje exige que el este sea manifestado de manera inequívoca, “mediante un acto afirmativo” que dé cuenta con claridad de la voluntad del titular. Sin embargo, se requieren mayores resguardos para evitar que la norma sea vulnerada a través de utilización de formularios pre-llenados u otras medidas similares.

En seguida, manifestó que en la iniciativa del Ejecutivo se desarrolla el principio de proporcionalidad. Connotó que la redacción del principio hace referencia al tiempo “necesario” de conservación, luego del cual los datos deben ser cancelados o anonimizados. Recalcó que hace falta establecer un límite máximo supletorio, luego del cual deba requerirse la autorización legal o consentimiento del titular.

En relación al derecho a la portabilidad, indicó que si bien resulta positiva la inclusión de este nuevo derecho, la iniciativa del proyecto establece requisitos excesivos para su aplicación. Se exige que el titular haya entregado sus datos personales directamente al responsable, excluyendo la posibilidad de ejercer el derecho a la portabilidad respecto de datos transferidos desde un tercero. También se exige que se trate de un “volumen relevante de datos”, lo que puede restringir arbitrariamente el ejercicio del derecho. Por último, recordó que el proyecto permite exigir un pago por los costos de ejercer la portabilidad. Esto contrasta con la gratuidad con que cuentan el ejercicio de los demás derechos contenidos en la ley, relegándolo a un estatus disminuido respecto de éstos.

Luego, hizo referencia al tratamiento automatizado de grandes bases de datos. Consideró que la redacción que propone el Mensaje parece autorizar el uso indiscriminado de datos personales con el fin de perfilar el comportamiento de sus titulares, sin necesidad de recabar un consentimiento previo. El proyecto tampoco permite a los titulares delimitar la toma de decisiones a través de perfilamiento revocando su consentimiento con posterioridad.

Agregó que en cuanto al tratamiento de datos de geolocalización, la iniciativa del Ejecutivo ciñe el tratamiento al principio del consentimiento informado y previo, y autorizando su revocación, pero sin considerar la posibilidad de solicitar la eliminación total de su información previamente recogida.

En relación a la Transferencia internacional de datos personales, indicó que el artículo 27 letra d) del Mensaje supone que no se requiere que el país receptor cuente con un estándar mínimo de protección de datos personales. El artículo 28, por su lado, entrega total discrecionalidad a la Agencia para autorizar la transferencia de datos cuando el país no cuenta con niveles adecuados de protección.

Estimó relevante poner atención al régimen de sanciones propuesto por el Ejecutivo. Destacó que las multas asignadas para cada tramo parecen muy bajas para asegurar un efecto realmente disuasivo.

Señaló que las excepciones a la aplicación de la ley (artículo 57 del proyecto de ley del Ejecutivo), contiene un listado de entidades públicas a las cuales no se aplicarán sus disposiciones, tales como el Congreso Nacional, el Poder Judicial y los organismos dotados de autonomía constitucional. Particularmente complejo resulta exceptuar al Servicio Electoral de la aplicación de la ley, pues sus funcionen implican un tratamiento masivo de datos personales.

Aseveró que las disposiciones transitorias contenidas en el proyecto antes mencionado concede un período excesivamente largo de adecuación respecto de las bases de datos constituidas con anterioridad a la entrada en vigencia del proyecto, un plazo total de cinco años.

Finalizó su intervención mencionando que el Mensaje no hace mención a una serie de materias que requieren ser abordadas para salvaguardar los derechos de las personas, tales como el *browser tracking*, la protección de metadatos y la regulación de retención de metadatos.

En una sesión posterior, **el Presidente de la Comisión, Honorable Senador señor Harboe** ofreció la palabra en primer lugar **al Presidente de la Cámara Chilena Norteamericana de Comercio (AMCHAM), señor Guillermo Carey.**

El señor Carey comenzó su presentación señalando que la organización que representa se ocupa de los intereses que derivan de las relaciones comerciales entre Chile y Estados Unidos. Agregó que en la actualidad cuentan con quinientos sesenta miembros.

Manifestó que la experiencia de muchos de los asociados a AMCHAM puede contribuir a enriquecer el presente debate y resaltar la importancia de tener un adecuado sistema de protección de datos personales, acorde con la modalidad en que se transan productos y servicios en la actualidad, que permita el desarrollo de nuevos emprendimientos a nivel internacional, respetando los derechos fundamentales de las personas.

Explicó que como Cámara de Comercio han participado activamente en las diversas instancias de discusión en torno a los múltiples esfuerzos legislativos que han buscado actualizar la ley N° 19.628 sobre Protección de la Vida Privada. En todas ellas han señalado que la industria y el comercio, no ven la regulación como una amenaza y la ausencia de regulación como una ventaja. Muy por el contrario, el escenario que sí es percibido como una desventaja, es uno donde exista una regulación que no sea clara, y que no permita un cierto grado de predictibilidad de las decisiones comerciales.

Precisó que sobre esta materia, Chile se encuentra ante la oportunidad de discutir y adoptar una actualización de la ley N° 19.628 sobre Protección de la Vida Privada que concluya en un marco normativo moderno y adecuado, tanto para la protección de los datos personales como para la generación e impulso de la economía y la innovación basada en datos.

Dado lo anterior, procedió a efectuar, las siguientes consideraciones que son relevantes para un proyecto de ley de este tipo:

1.- Existen varios sistemas de protección de datos personales a nivel internacional, que pueden lograr el mismo nivel de resguardo que se pretende. Junto con la normativa de la Unión Europea, existen otros estándares y ejemplos a seguir como el estándar OECD y APEC. Destacó que cuando hablamos de poner al día a nuestro ordenamiento estamos pensando que ello constituye un elemento habilitante para promover el libre comercio.

Agregó que en países como Argentina o Uruguay, que cuentan con la legislación adecuada, no necesariamente han aumentado las transacciones o las empresas de comercio electrónico.

Hizo presente que el mundo se está moviendo a una convergencia de nuevas tecnologías y hacia la irrupción de la inteligencia artificial, *Big data,* e *internet* de las cosas. Aseguró que la discusión del presente proyecto es relevante para que nuestro país esté al día, resguardando los intereses de las personas.

Recalcó que se deben considerar las realidades específicas de cada sector, evitando crear un modelo único de protección de datos. Para resolver lo anterior, sostuvo que deben crearse códigos de conducta sectoriales sancionados por la autoridad.

Consignó que la nueva legislación debe evitar la excesiva burocratización en los procesos de transferencia de datos que afecten el libre comercio, resguardando los derechos de los titulares de datos. Subrayó que es importante que se establezcan ciertas cláusulas tipo o determinados mecanismos que faciliten la transferencia de datos.

Abogó por un sistema que considere los avances de la técnica, que permitan la evolución tecnológica y además se cuente con una autoridad idónea que sea independiente, que sea capaz de generar este diálogo con los distintos actores para ir dándole la flexibilidad que se requiere a la legislación en estas materias.

Respecto a la autorregulación, recomendó que la legislación incorpore incentivos para promover la creación de códigos de conducta y mecanismos de autorregulación por parte de la industria. Esta forma de regulación ha demostrado ser un poderoso complemento para la ley.

Luego, indicó que en un informe del año 2015, sobre el rol y utilidad de la autorregulación en el resguardo de los intereses de los consumidores, la OCDE concluyó que ésta reporta grandes ventajas, tales como, mayor flexibilidad y rapidez para llenar vacíos regulatorios y modernizar la regulación; mayor grado de experticia técnica a la hora de regular y resolver controversias; menores costos administrativos para todos los actores, incluido el Estado; y favorece un mayor grado de compromiso con la ética y cumplimiento de las normas por parte de las empresas, pues al ser diseñada por la propia industria, ésta se ve comprometida en su éxito.

Por lo tanto, aseguró que les parece esencial promover códigos de conducta, buenas prácticas y autonomía de la voluntad entre las empresas y las personas, incluyendo la existencia de acuerdos sectoriales, convenios administrativos o decisiones de empresa que permitan incentivar el cumplimiento de la ley haciéndose cargo de las particularidades de la actividad o industria del controlador. Enfatizó que el Estado debería actuar como un depositario y fiscalizador del cumplimiento de los códigos de conducta, los que deberían estar asociados a atenuantes de responsabilidad.

Asimismo, sugirió la incorporación de un tercer actor, que es el intermediario. Expresó que es recomendable reconocer y definir el rol del intermediario de datos, quien por su naturaleza pone a disposición un servicio tecnológico neutro que involucra tratamiento de datos recopilados por terceros.

Estimó pertinente, debido a la convergencia de medios, que los actores relacionados con la infraestructura de telecomunicaciones no sean medidos con la misma vara que los responsables o los encargados.

En relación a la transferencia internacional de datos, reiteró que se debe evitar la burocratización de los procesos para no entrabar el libre comercio, respetando los derechos de las personas como también la libre circulación de los datos personales. Agregó que el cuidado de este equilibrio es particularmente relevante en la regulación de las normas sobre transferencia internacional de datos personales.

Aseveró que no se debe ignorar que existen otros modelos para garantizar la compatibilidad de los sistemas de protección de datos personales, incluyendo revisiones ex post de la autoridad, tal como ocurre en Singapur, México y Canadá.

Propuso incluir instrumentos paralelos a un estándar de adecuación, como cláusulas contractuales modelo, reglas corporativas vinculantes o acuerdos internacionales, que son flexibles y no generan la inclusión-exclusión, como lo hace la adecuación.

Apuntó que en un sistema donde las bases de licitud del tratamiento son únicamente la autorización del titular o de la ley, las excepciones a la obligación de obtener consentimiento dotan a la ley de sensatez y de conexión con la realidad. Añadió que tanto en la vida diaria como en el tráfico jurídico y comercial, existen escenarios donde es razonable que el consentimiento se haya prestado, o no tenga por qué requerirse, o sea en la práctica imposible de conseguir, debiendo tratarse los datos de igual forma.

Destacó que una ley que no admite excepciones, o que contempla pocas o las define pobremente (como la actual ley de protección de datos) se transforma finalmente en una norma que no es aplicada, desfavoreciendo precisamente a quienes pretendió beneficiar. Por ello, estimó como esencial contar con un catálogo concreto de excepciones a la obligación de obtención del consentimiento para el tratamiento de datos.

Finalizó su intervención sosteniendo que se debe dar cierto espacio a excepciones que permitan ir adaptando la institucionalidad a la nueva realidad.

A continuación, **el Presidente de la Comisión, Honorable Senador señor Harboe** ofreció la palabra **a los representantes de la Asociación de Aseguradores de Chile A.G.**

En representación de esta entidad, hizo uso de la palabra, **el abogado Francisco Serqueira**, quien comenzó su intervención indicando que en Chile existen 62.000.000 de coberturas de seguro. Agregó que el sector asegurador ha alcanzado una cifra cercana al 5% del Producto Interno Bruto.

Afirmó que lo anterior corresponde a la penetración y la densidad aseguradora en el país. Aseveró que el seguro ha ingresado a distintas capas de la sociedad y se ha transformado en un instrumento no solo económico, legal, sino que también de protección social.

Sostuvo que el contrato de seguro debe contener una serie de datos personales. Por lo mismo, puntualizó que la industria aseguradora trabaja con muchos datos.

Bajo ese prisma y dada la importancia de la materia, señaló que ambas iniciativas constituyen una actualización importante para que nuestro país cuente con normas legales de estándar internacional en el tratamiento de datos personales.

Agregó que en el ámbito asegurador, se requiere que esta regulación concuerde primeramente con la penetración y densidad del “seguro” como elemento de protección social; y con los períodos precontractuales, contractuales, y de liquidación de pagos y siniestros.

Luego, consignó que al organismo público de protección de datos (Agencia) se le otorgan facultades para dictar instrucciones y normas obligatorias, fiscalizar, requerir información a los fiscalizados, resolver reclamos, y aplicar sanciones. Idénticas facultades tiene la Superintendencia de Valores y Seguros en su ámbito relacionado con el contrato de seguros y las empresas aseguradoras.

Expresó que las normas de dicha Agencia, aplicables al sector de seguros, deben ser dictadas mediante Normas Conjuntas.

Añadió que en el proyecto del Ejecutivo, el tratamiento de datos se rige por “principios” (Art. 3º), y se responde legalmente por el cumplimiento de éstos. Por lo anterior, estimó que el contenido y alcance de los éstos se exprese exhaustivamente en la ley, evitando “legislaciones administrativas”.

Por ejemplo, en la iniciativa del Ejecutivo, específicamente en su artículo 3°, letra d), se señala: “Principio de calidad: los datos personales deben ser exactos…”. A continuación se dice quienes realicen el tratamiento de los datos son “legalmente responsables del cumplimiento de los principios”, siendo éste el principio de responsabilidad.

Dado este ejemplo, solicitó que en el principio de calidad, sea la propia ley la que establezca que si los datos son recogidos directamente del titular, de su representante, de su mandatario, del proponente, o del contratante, se consideren “exactos”, haciendo de esa forma posible el principio de responsabilidad.

Admitió que lo anterior es relevante, ya que en la medida que seamos capaces de delimitar los principios, se limitará cualquier sobre medida de discrecionalidad administrativa.

Enfatizó que si estuviésemos tratando un tema de carácter penal, debiésemos decir que hay que tratar de evitar generar una especie de ley penal en blanco, en donde el tipo termina siendo acotado, definido por instancias no legislativas.

Expuso que el que no cumple con los principios es sancionado. Aseveró que incluso se permite que la autoridad administrativa suspenda o impida en forma definitiva que una determinada entidad continúe haciendo tratamiento de datos.

Reiteró que la industria aseguradora y el contrato de seguro constituyen un conjunto de datos. Precisó que el solo hecho de visualizar que un incumplimiento de principios pueda llevar a la suspensión del tratamiento de datos significa suspender a una actividad aseguradora legítima.

Recomendó tratar de ser lo más exhaustivo posible en la enunciación de los principios, dado que éstos son, en definitiva, sobre los cuales se construye toda la legislación.

Atendida la naturaleza del contrato de seguro, connotó que la legislación especial reconoce que existe toda una etapa previa a la perfección del contrato de seguro. Consecuentemente, en las excepciones al consentimiento, debe reconocerse la existencia de etapas precontractuales que derivan en recoger, procesar, almacenar, comunicar y transmitir datos del titular, sean contratantes, asegurados, o beneficiarios.

Concluyó su exposición solicitando que se agregue un artículo al proyecto de ley, que incorpore una nueva disposición al Decreto con Fuerza de Ley N° 251, de 1931, en los siguientes términos:

“Las entidades aseguradoras podrán establecer bases de datos comunes que contengan datos de carácter personal para la liquidación de siniestros y la colaboración estadístico actuarial para permitir la tarificación y selección de riesgos y la elaboración de estudios de técnica aseguradora. La cesión de datos a las citadas bases no requerirá el

consentimiento previo del afectado, pero sí la comunicación a éste de la posible cesión de sus datos personales a bases de datos comunes para los fines señalados, con expresa indicación del responsable, para que se puedan ejercitar los derechos de acceso, rectificación y cancelación previstos en la ley.

También podrán establecerse bases de datos comunes cuya finalidad sea prevenir el fraude en el seguro sin que sea necesario el consentimiento del afectado. No obstante, será necesaria en estos casos la comunicación al afectado, en la primera introducción de sus datos, de quién sea el responsable de la base de datos y de las formas de ejercicio de los derechos de acceso, rectificación y cancelación.”.

A continuación, **el Presidente de la Comisión, Honorable Senador señor Harboe,** ofreció la palabra a **la integrante de la Comisión de Propiedad Intelectual del Colegio de Bibliotecarios de Chile, señora Claudia Cuevas**.

Al iniciar su presentación, **la señora Cuevas** agradeció la invitación cursada para tomar parte en esta discusión. Remarcó la tradición de las bibliotecas respecto al resguardo de los datos, la confidencialidad, la administración de los mismos y la gestión del conocimiento.

Señaló que le parece fundamental que se armonice el articulado del proyecto con el derecho al olvido. Destacó la importancia de enfatizar ciertos conceptos, otorgarles una definición más acabada y acotar su real significado y alcance.

Manifestó que se debe garantizar el acceso permanente a la información, sobre todo a aquellos que son titulares de derechos de datos. Además, subrayó que el mismo debe ser gratuito.

Expuso que se debe precisar con claridad quiénes son los responsables y los intermediarios de datos. Agregó que se debe informar oportunamente al titular si sus datos van a ser modificados o actualizados. Sostuvo que éste debe autorizar el cambio.

Igualmente, estimó que se debe comunicar si la cesión o la transferencia de datos se efectúen en otras bases de datos que no sean públicas.

Sugirió que en la ley se establezca cuál será la institución pública que será la responsable de definir el registro actualizado de las instituciones que están con niveles adecuados de protección de datos.

Propuso que el Estado vele y cautele, explícitamente en la ley, el derecho de todos los ciudadanos a acceder a toda la información y conocimiento generado y producido con fondos públicos. De tal forma, las publicaciones que resulten de investigaciones promovidas por universidades y cualquier otra entidad de investigación que hayan recibido financiamiento público estén disponibles de forma gratuita.

Aseveró que no es posible que dichas instituciones estén afectas a dobles pagos (sueldos de investigadores y compra y/o suscripción del artículo o revista donde las investigaciones son diseminadas) y, menos aún, que la mencionada información esté disponible previo pago por parte de la Biblioteca, ciudadano o lector.

Por otra parte, afirmó que no parece conveniente que los datos inferidos sean transferibles (por ejemplo, historial de compras de Amazon, fichas médicas u otros), por cuanto, la generación de nuevos datos a partir de algoritmos de los datos compilados apuntan a predicciones que no necesariamente representan al titular de datos o que, en otros contextos ajenos a donde se produjeron, pueden inducir a error o, simplemente, a datos distintos resultado de interpretaciones inducidas.

Recalcó la relevancia de contar con profesionales idóneos en la Agencia de Protección de Datos Personales para el tratamiento y gestión de información, de tal forma, que el almacenamiento y recuperación de datos (bibliotecarios, bibliotecólogos) responda a estándares y metodologías que permitan no solo la interoperabilidad y permanencia en el tiempo, sino también, compartir y enriquecer los datos, en particular, para aportar a la eficiencia de la administración de archivos, sobre todo, a nivel gubernamental.

Finalmente, manifestó que la Asociación Profesional que representa, defiende el acceso sustentable y equitativo a la información, derecho humano garantizado en el artículo 19 de Declaración Universal de Derechos Humanos, así como, el buen uso de los datos de las personas; así también, promueve la importancia de garantizar el acceso público a la información y protege las libertades fundamentales, de conformidad con las leyes nacionales y los acuerdos internacionales (Objetivo de Desarrollo Sostenible 16.10 de la Agenda 2030 para el Desarrollo Sostenible) en todas las bibliotecas de nuestro país y del mundo, así como, en todas las bibliotecas de acceso público que, sin fines de lucro, garantizan el acceso a la información, la cultura, el esparcimiento y el conocimiento.

A continuación, **el Presidente de la Comisión, Honorable Senador señor Harboe** ofreció la palabra **al abogado del Estudio Jurídico Ferrada-Nehme, señor Víctor Andrade.**

El señor Andrade agradeció la invitación y consignó que su exposición tratará sobre la portabilidad de datos. Explicó que éste es un derecho que se consagra en ambos proyectos de ley.

Afirmó que la portabilidad de datos es uno de los tópicos legales en que de forma más clara se aprecia la intersección entre la protección de datos personales, el derecho de la competencia y la regulación económica.

Expresó que hay una diferencia fundamental cuando entendemos portabilidad de datos respecto de otro tipo de portabilidad. Señaló que el ejemplo más común lo constituye la del número telefónico, pero éste no sirve para entender la portabilidad de datos.

Agregó que la portabilidad en materia de datos personales busca reafirmar una identidad digital.

Reflexionó sobre la situación en caso que se quisiera utilizar un historial de compras de libros de Amazon para que se forme un perfil en relación al comportamiento de pago. No son competidores, no busca cambiar de servicio pero sí podría ser una nítida aplicación de la portabilidad de datos.

Señaló que los casos de portabilidad conocidos a la fecha, parten de la existencia de un producto o servicio particular altamente estandarizado.

Luego, destacó que en la portabilidad de datos, no existe a priori un servicio o producto en particular cuyos datos pretenden ser portados y recibidos, por lo que los usos de la portabilidad pueden ser innumerables.

Aseveró que incluso se podría dar la creación de un mercado secundario de gestión de data portable, en el que participen *brokers* y agregadores de datos.

Añadió que el *Big data*, la portabilidad de datos y las notificaciones de vulneración a la seguridad de protección de datos personales forman una triada de las obligaciones tecnológicas que ambas iniciativas incorporan a nuestra legislación.

Manifestó que la portabilidad se incluye tanto como derecho, y como sistema de su ejercicio, entendiendo que es un derecho particular que se añade al catálogo de derechos ARCO.

Observó que no hay mucha diferencia de tiempo entre lo que pueden ser los aciertos y errores de la normativa europea y las posibilidades que existen en la normativa nacional de incluir la portabilidad.

Sostuvo que la portabilidad como caso de prueba, desde el punto de vista de acusaciones por protección de datos personales o por abusos en el ámbito del derecho de competencia es del mismo nivel de incertidumbre en cualquier parte del mundo.

Asimismo, hizo presente que si uno desglosa cuál es el derecho a portabilidad, en estricto rigor son dos, a saber: el derecho a recuperar la información, es decir, a solicitar y recibir la información que se tiene de una persona; y otro, el más complejo desde el punto de vista de cómo se puede realizar, es el derecho a transferir directamente la información de un responsable a otro.

Agregó que como ambas iniciativas siguen una línea parecida a lo que es el Reglamento General Europeo de Protección de Datos, conviene analizar las opiniones que se han visualizado respecto del alcance en la portabilidad.

Seguidamente, señaló que los problemas que se enfrentan en Chile son similares a los del derecho comunitario europeo. Connotó que el primer conflicto es la portabilidad únicamente de datos proporcionados por el titular. Señaló que la norma hace referencia a los datos personales que hayan sido entregados directamente por el titular. Aseveró que la virtud de la portabilidad es que los registros de actividad y toda la información que se origina respecto a una persona, pueda ser portado.

Consignó que la legislación europea ha precisado que hay dos tipos de datos que se generan sobre las personas, uno corresponde a los observables, y otro puede ser, por ejemplo, el *scoring* que se le otorga a una persona por su capacidad de pago. Recalcó que este último no debiese ser objeto de portabilidad, porque para el titular es pernicioso lo que puede suceder si de ello toman conocimiento más personas, porque la predicción tiene que estar basada en determinados antecedentes que son esencialmente verificables.

Concluyó su intervención subrayando que la portabilidad no puede superar o reemplazar proyectos de ley que dicen relación con interoperabilidad de plataformas, ya que para ello existen iniciativas legales específicas, como por ejemplo, la de plataforma de cuenta común interbancaria y de plataforma de acceso bancario.

A continuación **el Presidente de la Comisión, Honorable Senador señor Harboe** ofreció la palabra **al asesor de la Fundación Jaime Guzmán, señor Héctor Mery.**

El señor Mery comenzó señalando que no es fácil encontrar un fundamento dogmático explícito a la tutela de los datos personales en Chile.

Expuso que el artículo 19, número 4 de nuestra Carta Fundamental se refiere a las categorías "honra" y "vida privada". Reconoció que si bien existen en la Constitución, no bastan por sí mismas para encontrar una respuesta a este problema.

Indicó que en España se reconoce a las personas el derecho fundamental a la intimidad, del cual emana el derecho de la persona al control de sus datos personales.

Asimismo, recordó que, en discusiones previas sobre este proyecto, y en la iniciativa de reforma constitucional tramitada paralelamente a esta iniciativa, se busca configurar la protección de datos como "un derecho fundamental".

Agregó que se deduce por algunos que, al ser un "derecho fundamental", su titularidad queda reservada a las personas naturales. Esa conclusión, argumentó, me parece excesiva, si bien reconocemos que es difícil suponer su legitimación a las personas jurídicas.

Subrayó que la ley no debiera definir esas categorías, pues su contenido es en esencia constitucional. Se mostró partidario de permitir que la hermenéutica y los principios constitucionales definan esta materia.

Asimismo, sostuvo que la definición de la tutela de datos personales corresponde a una dimensión y prolongación de la libertad. Respecto a la titularidad de este derecho, se preguntó si las personas jurídicas tienen derecho a la privacidad.

Manifestó que, desde el punto de vista práctico, las personas jurídicas son creadas principalmente para actuar de manera pública en materias comerciales, el resto de sus datos son por esencia públicos y, finalmente, no tienen datos personales sensibles (nombre, rut y domicilio son todos públicos, no tiene raza, género, antecedentes políticos ni de salud, por lo que lo único relevante es su comportamiento económico).

Hizo presente que, por lo anterior, sería contraproducente establecer un derecho a la privacidad en materia económica, ya que iría contra la esencia de la necesaria transparencia en los

actos de comercio y sobre todo para la estabilidad y confianza del sistema económico en su conjunto.

Consideró que siempre es bueno saber con quién haces negocios. Recalcó que no existiría un bien jurídico protegido en la privacidad de las personas jurídicas, que a menudo deben moverse en la esfera pública. Estimó que, en este caso, además es mucho más relevante la protección de la confianza en los mercados, para lo cual la información de los actores es clave.

Expresó que, sin perjuicio de lo anterior, no es imposible suponer la aparición de un caso en que sería posible la protección de la privacidad de las personas jurídicas. Añadió que se deben evitar definiciones legales que no admitan esta posibilidad.

En cuanto a los sesgos en la regulación, parece inconveniente adoptar una aproximación que defina categorías en esta ley que pudiere pugnar, o prevalezcan derechamente, sobre otros derechos y categorías que la Constitución también cautela y ampara, que el Estado también debe "promover y respetar", tales como, la libertad de empresa, libertad de expresión, y la prohibición de censura previa.

Desde otra perspectiva, consideró que se debiera adoptar un régimen dogmático e institucional que asegure igual tutela a estos datos, sin importar que el sujeto que hiciere el tratamiento de datos sea el sector público o el sector privado.

Asimismo, sugirió revisar la conveniencia de fijar una regla de competencia para establecer responsabilidades de personas domiciliadas y que operan en el extranjero. La ley chilena es muy cuidadosa respecto de la pretensión de obligatoriedad en territorio extranjero, y no parece haber buenas razones para innovar en esta materia.

Respecto a quién debiera ser el responsable institucional de la protección de datos, explicó que se han suscitado diferencias sobre si debiera estar a cargo de una agencia dependiente o ligada al Ministerio de Hacienda, o hacer que esta competencia recaiga en el Consejo para la Transparencia. Estimó que el mencionado Consejo, en su desempeño histórico, ha pronunciado resoluciones que, aunque reconocen su sesgo esencial (publicidad y transparencia), permiten adjudicarle esa responsabilidad, lo que parece mejor que constituir un organismo sin precedentes.

A continuación, **el Presidente de la Comisión, Honorable Senador señor Harboe** ofreció la palabra **al Vicepresidente de la Fundación Hacer Chile, señor Rodrigo León.**

El señor León comenzó su presentación manifestando que el proyecto del Ejecutivo consta de una parte orgánica y otra normativa. Respecto a esta última indicó que se debe tener precaución respecto a la implementación de nuevos principios que escapan a lo que es el sistema jurídico nacional.

Expresó que la ley N° 19.628 sobre tratamiento de datos personales, que data de 1998, tiene por objeto la regulación del tratamiento de datos personales de personas naturales, es decir, la comunicación, trasmisión, almacenamiento y uso de dichos datos. El dato personal es todo dato que sirva para identificar a una persona determinada, como: el RUT, la dirección, la patente del autor, su cadena genética, su huella digital, etc.

Agregó que la reciente iniciativa legal presentada por la Presidenta de la República, mediante boletín N° 11.144-07 y la moción parlamentaria contenida en el boletín 11.092-07, establecen una modificación radical al régimen actual de tratamiento de datos personales.

Por de pronto, en el proyecto de ley del Ejecutivo se establece una autoridad administrativa con facultades de fiscalización y sanción a los responsables de base de datos: la Agencia de Protección de datos personales. Esta autoridad, hoy inexistente en Chile, es un organismo común en los países con sistema de protección de datos, Chile era de las excepciones al no contar con uno.

Se mostró contrario a que el Consejo para la Transparencia tome para sí el control de la protección de datos personales. Por otra parte, afirmó que el dato sensible debe ser regulado. Aseveró que en la ley chilena actual, el dato sensible no reúne esa característica, sino que es un dato personal cualquiera y no tiene una regulación especial.

Consignó que es improcedente que el proyecto del Ejecutivo consagre el dato genético, biométrico, porque caben dentro de la categoría general de dato sensible.

Asimismo, consideró relevante la regulación que hace la iniciativa del Ejecutivo respecto a los menores de edad.

Luego, manifestó que en nuestro país no se encuentra regulado el derecho al olvido y es fundamental que se haga.

Reseño que la ley francesa de datos personales instituye sanciones por 10.000 EUR. Declaró que el proyecto de ley en discusión establece multas que pueden alcanzar la suma de US$ 1.000.000. Opinó que no hay ninguna proporcionalidad en ellas.

Señaló que extender la ley de protección de datos personales a personas jurídicas no es correcto. Recordó que ello no lo aplica ningún país. Subrayó que, salvo excepciones muy específicas, la protección de datos personales está asociada a los temas de privacidad.

En relación a la regulación transfronteriza de datos, connotó que existe una deuda respecto del Acuerdo de Cooperación con la Unión Europea. Recalcó que debe seguirse en esta materia el principio internacional de la reciprocidad.

Seguidamente, señaló que si se busca hacer un resumen de las nuevas disposiciones, habría que destacar las siguientes:

1. La nueva ley parte estableciendo unos nuevos derechos reunidos en los denominados derechos “ARCO”, es decir, los derechos de Acceso, de Rectificación, de Cancelación y de Oposición. Este conjunto de derechos podrán ser ejercidos por vía administrativa en forma muy rápida -actualmente los derechos de habeas data se ejercen judicialmente en procesos largos y complejos que casi nunca se han usado desde 1998-. La vía administrativa se seguirá ante esta nueva Agencia de protección de datos personales. Adicionalmente se reconoce un derecho de portabilidad de datos personales.

2. El proyecto de ley distingue categorías de datos personales en forma clara, cosa que hoy no existe. Recordemos que el dato personal siempre está asociado a una persona natural no a personas jurídicas – salvo una excepción muy específica en la ley actual -. Las nuevas categorías de datos personales que tienen gran diferencia con el sistema actual están relacionadas con: los datos personales generales cuyo uso requiere consentimiento previo expreso claro del titular del dato; los datos personales sensibles que actualmente están regulados en la ley como los datos personales generales, en el proyecto la regulación del dato sensible es bastante más engorrosa, en particular datos personales biométricos, biológicos y de salud. Adicionalmente se regulan los datos personales de niños y adolescentes, según la ley distinguiendo aquellos menores de 14 años y aquellos entre 14 y menos de 18 años.

3. El nuevo procedimiento administrativo para ejercer los derechos “ARCO” y la nueva categorización de datos personales en datos personales es muy diferente al actual sistema, mucho más libre en que no existen sanciones ni responsabilidades específicas para los responsables de bases de datos personales.

4. Respecto a las nuevas responsabilidades de las empresas que manejan bases de datos personales, es decir todas las empresas, es importante poner de relieve que el proyecto viene a implementar una regulación del mercado del tratamiento de datos personales

totalmente nuevo, imponiendo una serie de obligaciones de comunicación, de custodia, seguridad y eliminación de datos personales. Por ejemplo será obligatorio tener publicada una casilla electrónica o vía similar de comunicación pública para reclamos además de sendas políticas de privacidad de las empresas. La fiscalización, hoy inexistente, será muy invasiva, y podemos sin lugar a dudas calificar a la Agencia de datos personales como el SERNAC de la privacidad. El deber de custodia y seguridad será sancionable con multas como todo otro derecho "ARCO". En forma desafortunada el proyecto hace heredable todos estos derechos lo que a nuestro entender es absurdo.

5. El proyecto ordena el actuar de los servicios públicos en materia de intercambio de datos personales entre ellos además de regulaciones especiales en materia de eliminación o derecho al olvido de datos relacionados con responsabilidades penales, administrativas o civiles, poniendo como plazo máximo 5 años de mantención en repositorios.

6. Asimismo, es necesario poner de relieve que la nueva normativa establece infracciones que hoy no existen en la ley. Las infracciones se categorizan en tres clases, leves, graves y gravísimas, sanciones que constituyen multas a beneficio fiscal que pueden ir de una U.T.M. a 5000 U.T.M., en caso de reincidencia estas multas se pueden multiplicar por tres. Adicionalmente la prohibición de tratar datos personales.

7. Por otro lado, todo lo tocante a la relación entre el responsable de la base de datos y los usuarios está muy normada. La regulación actual es casi inexistente, en cambio en el proyecto de ley los intercambios de comunicación entre el responsable de la base de datos y los titulares de los datos personales es extremadamente importante, por de pronto como se señaló, se establece la obligación a los responsables de base de datos a tener un correo electrónico de contacto obligatorio de tener políticas de privacidad obligatorias. La regla general es que no se podrá tratar datos personales sin consentimiento del titular, concepto técnico en la ley que se considera como la manifestación de voluntad libre, específica, inequívoca e informada mediante la cual el titular de datos, su representante legal o mandatario, según corresponda, autoriza el tratamiento de los datos personales que le conciernen.

8. Asociado a la relación empresa de base de datos y titular, la ley considera la existencia de certificaciones de modelos de prevención ante la Agencia de protección de datos personales. Es decir se deben hacer certificaciones de modelos de prevención por la Agencia de protección de datos que tendrán duración de tres años de aprobarse el proyecto de ley tal cual.

Terminó enfatizando que el proyecto de ley en discusión es fundamental para el futuro de nuestro país.

El Presidente de la Comisión, Honorable Senador señor Harboe ofreció la palabra **al Consejero del Instituto Chileno de Derecho y Tecnología, señor Carlos Reusser.**

El señor Reusser comenzó su presentación agradeciendo en nombre del Instituto Chileno de Derecho y Tecnologías la oportunidad que se les brinda de exponer sobre un tema apasionante y que, de aprobarse, será uno de los avances más sustantivos en materia de derechos fundamentales desde el retorno de la democracia, pues pondría fin a una debilidad estructural de nuestro sistema de derechos que se arrastra por demasiados años.

Manifestó que el nudo de la cuestión radica en lo siguiente: ¿De qué nos sirve preconizar que en la Constitución existe el derecho al trabajo, a la educación o la vivienda si alguien (que no sabrás quién), cree saber algo de ti (que no sabrás qué) y que en definitiva tomará una decisión arbitraria a tu respecto, dejándote en la indefensión?

Expresó que ésta es la realidad de los chilenos hoy en día y no es culpa de los tiempos o del avance tecnológico, sino que es el resultado de una legislación deficiente creada no para proteger a la gente contra los abusos que se cometen a través del tratamiento automatizado de la información, sino para regular el mercado de datos: no por nada la ley Nº 19.628 se conoció por muchos años como la “Ley DICOM”.

Destacó que el objetivo de estos proyectos de ley es claro. Buscan que nuestro país alcance los estándares vigentes en la materia y que por ello sea reconocido internacionalmente, es decir, que en definitiva, la OCDE, la Unión Europea y otros entidades de carácter internacional reconozcan que Chile es un país con un nivel adecuado de protección de datos, lo que redundará tanto que en los chilenos dispondrán de un amparo legal efectivo ante tanto abuso, como que el país también pueda ser receptor de datos personales de ciudadanos de otras latitudes, en operaciones de comercio o prestación de servicios transfronterizos, sin dilaciones ni trabas excesivas.

Luego, precisó que esperan que este sea el inicio de una floreciente y reconocida industria de servicios especializados en materia de datos personales, como son las certificadoras de datos, las aseguradoras de datos y la industria de la seguridad de la información en general, sin perjuicio de la actividad que desarrollen también los proveedores de infraestructura tecnológica.

Consignó que el problema radica en que con el contenido de los proyectos de ley en actual trámite, no se cumple con los

requisitos que permitan alcanzar el objetivo recién esbozado, es decir, que después de un largo y costoso esfuerzo de los colegisladores y todos los involucrados, podríamos perfectamente llegar a la misma situación en que empezamos, pues el proyecto del Ejecutivo tiene un defecto crítico para estas pretensiones, que nos excluye desde la partida como acreedores del reconocimiento “país con un nivel adecuado de protección de datos”: no desarrolla de forma adecuada la debida independencia de la autoridad de control, sino que solo construye un sucedáneo del Ministerio de Hacienda que no resistirá el análisis de, entre otros, los comités de protección de datos de las entidades internacionales.

Hizo presente también que el derecho a la protección de datos no es la otra cara del derecho al acceso a la información pública. Agregó que la transparencia y el acceso a la información pública son líneas de acción que se han desarrollado en base a la necesidad creciente de los Estados de contar con herramientas para luchar contra la corrupción, en cambio, el derecho fundamental a la protección de datos es un metaderecho que tiene por objeto proteger a todos y cada uno de los derechos fundamentales y legales de las personas. Precisó que no hay ninguna proporción entre la importancia y rol de uno con el del otro, no son equiparables y no es un asunto a empatar como suelen presentarlo quien hacen este tipo de falsas analogías en que incluso reprochan supuestos privilegios de quienes se ocuparían de la protección de datos contrastándolo con las atribuciones, no menores, del Consejo para la Transparencia.

Respecto de los proyectos de ley refundidos, expresó que centrará su exposición en cinco ideas:

1. La incorrecta apelación al derecho a la vida privada.

Tanto el mensaje como el artículo 1° del proyecto del Ejecutivo apelan al derecho a la vida privada, pero los datos de la vida privada (o “privacidad” que llaman otros) no tiene relación con el contenido de estas iniciativas legales.

Agregó que si a una persona no la contratan en un trabajo porque se enteraron que ella demandó a su empleador anterior, lo que se vulnera es el derecho al trabajo, no a la vida privada.

Hizo presente que si una ISAPRE se niega a otorgar prestaciones de salud alegando preexistencias no declaradas en base a lo que una persona ha comprado en la farmacia, lo vulnerado es el derecho a la salud, no la vida privada.

Luego, connotó que si se usan los datos de afiliación sindical para hacer descuentos respecto de huelgas en las que un

sujeto no ha participado, entonces lo afectado es la libertad sindical, no la vida privada.

Opinó que a estas alturas se deben desterrar ideas y concepciones jurídicas de los años 80 del siglo pasado, pues desde hace mucho es claro que la vida privada solo es uno de los tantos derechos que pueden verse afectados, ni siquiera el más relevante de ellos.

Remarcó que en el estado actual lo importante de relevar, ya sea expresa o tácitamente, es la autodeterminación informativa, esto es la libertad de cada persona de hacer con sus datos lo que estime conveniente dentro del marco legal, y dicha autodeterminación se expresa en el derecho a la protección de datos personales que debería consagrar adecuadamente nuestro país.

2. Obligaciones internacionales de Chile en materia de datos personales.

Aseveró que no es efectivo lo sostenido por el Ministerio de Hacienda en sesión pasada en el sentido de que Chile solo tiene que responder internacionalmente, en materia de protección de datos, frente a los requerimientos de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) o que esta ley debe aprobarse como “un buen comienzo”.

Añadió que Chile pertenece tanto al sistema de la Organización de las Naciones Unidas y también a la Organización de Estados Americanos, y la primera de ellas ya ha emitido Directrices para la regulación de los archivos de datos personales informatizados en 1990 y luego una Resolución A/C.3/68/L.45/Rev.1 sobre el Derecho a la Privacidad en la Era Digital, en 2013.

A su vez, la Organización de Estados Americanos ha normado la materia tanto a través de la AG/RES. 2842 (XLIV-O/14) sobre acceso a la información pública y protección de datos personales como también estableciendo los Principios de la OEA sobre la Privacidad y la Protección de Datos Personales.

Pero si ello no fuera suficiente o por si las referencias parecieran vagas, un tratado vigente, el Acuerdo por el que se establece una Asociación entre la Comunidad Europea y sus Estados miembros, por una parte, y la República de Chile, por otra, publicado en el Decreto 28 de 2003, del Ministerio de Relaciones Exteriores, dice textualmente en el Artículo 202 «Las Partes acuerdan otorgar un elevado nivel de protección al procesamiento de datos personales y de otra índole, compatible con las más altas normas internacionales».

Se preguntó cuál es la más alta norma internacional en la materia. Respondió que es el Reglamento General de Protección de Datos que entra a regir el próximo año, aplicable a Europa, Argentina, Canadá, Israel, Nueva Zelandia, Uruguay a todo país que aspire al reconocimiento que ya hemos mencionado.

Recalcó que en esta materia es claro que nuestro país no ha honrado el Acuerdo y el Ministerio de Hacienda debería saberlo, particularmente considerando que dicho tratado internacional contempla que incluso los Estados se pueden excepcionar de su cumplimiento en materia de comercio o de servicios financieros si con ello protege de mejor manera la intimidad y los datos personales (art. 135).

En síntesis, sostuvo que no solo debe responderse ante los requerimientos de la OCDE, sino también con los tratados internacionales suscritos por nuestro país, sin perjuicio de las directrices de organizaciones internacionales sobre la materia.

3. Libertad de información y opinión versus protección de datos.

Señaló que el artículo 1° tanto del proyecto de ley del Gobierno como en la Moción parlamentaria se mantiene un anacronismo de la actual ley, como es establecer, en los hechos, una primacía de la libertad de información y de opinión por sobre el derecho a la protección de datos.

En el fondo, normativamente se le está dando un carácter de derecho absoluto a la libertad de opinión y de expresión, cerrándoles a los jueces las vías para solucionar asuntos complejos en que los derechos deben conciliarse o compatibilizarse.

Hizo presente que el nuevo Reglamento General de Protección de Datos de Europa establece claramente un deber de conciliación entre derechos y no relaciones de subordinación. Así lo dice el Considerando 153, que plantea que los Estados deben “conciliar las normas que rigen la libertad de expresión e información, incluida la expresión periodística, académica, artística o literaria, con el derecho a la protección de los datos personales”.

Esto tiene efectos prácticos muy importantes. Por ejemplo, un diario o periódico no puede estar en una situación de privilegio legal que le permita poner a disposición de público una noticia durante 20 años, cuando dicha noticia es agraviante para una persona o grupo de personas particulares, con la excusa de que tiene un estatuto jurídico especial por sobre la protección de datos de las personas, aun cuando los hechos relatados ya no sean noticia.

Sostuvo que es muy relevante que se distinga entre la libertad de información y de opinión de diarios o periódicos y las bases de datos que se construyan con dicha información, las que en todo caso deben quedar sujetas a la ley de protección de datos personales.

4. Diferencia arbitraria en el trato dependiendo de si quien vulnera el derecho a la protección de datos es un ente público o privado.

Expresó que el artículo 23 del proyecto del Gobierno contiene una disposición inexplicable y odiosa que implica que si quien deniega el ejercicio de los derechos reconocidos por la ley de protección de datos es un ente privado, puede acudir a la Autoridad de Protección de Datos en búsqueda de amparo, pero si quien vulnera los derechos de las personas es un organismo público, entonces debe tener el dinero suficiente para pagar a un abogado especializado y someter el asunto a las ritualidades y costos propios de un juicio, deduciendo un reclamo de ilegalidad ante las Cortes de Apelaciones respectiva.

Subrayó que nada justifica esta asimetría y, en la práctica, es poner a los ciudadanos de clase media y a los más pobres una barrera de acceso a la protección efectiva de sus derechos: la generalidad de la gente tiene dinero para vivir, pero no el suficiente como para sobrellevar los costos de un juicio (“pobreza legal”), por lo que tienden a aceptar lo que no deberían y, en los hechos, se les deja en la indefensión.

Añadió que la única razón que podría explicar el artículo 23 tiene que ver con un erróneo diseño institucional en el cual se deja a una Autoridad de Protección de Datos Personales, que carece de autonomía legal, bajo la supervisión del Presidente y la tutela directa del Ministerio de Hacienda (al que debe asesorar, por lo demás), subsumido dentro de la administración regular del Estado.

5. Falta de autonomía e independencia de la autoridad de protección de datos personales.

Manifestó que hay dos factores críticos de nuestra ley actual que la han separado durante todos estos años del reconocimiento internacional de país con un nivel adecuado de protección de datos: uno de ellos es la ausencia de un régimen de sanciones, cuestión que los proyectos solucionan bastante bien, y el otro es la ausencia de una autoridad de control independiente que se ocupe de la protección de datos.

Expuso que los proyectos de ley en análisis versan sobre protección de derechos fundamentales; en consecuencia es una iniciativa que, en principio, debería estar a cargo del Ministerio de

Justicia o del Ministerio Secretaría General de Gobierno, pero no del Ministerio de Hacienda, que tiene otros roles y fines, y menos aún que dicho Ministerio se reserve el rol de vaso comunicante con el Presidente de la República amparándose en que se tratan de una entidad técnica cuando se trata de un Ministerio eminentemente político, como todos los demás.

Explicó que contrariamente a lo que ha sostenido el Ejecutivo en otras sesiones, no es efectivo que muchos países establezcan en su legislación que la autoridad de protección de datos se relacione con el Ejecutivo, a través del Ministerio de Hacienda.

Connotó que solo hay un caso y es Nicaragua, quien no ha obtenido el reconocimiento de país con nivel adecuado de protección de datos, ni lo tendrán nunca en las actuales circunstancias, pues su falta de independencia se deriva de la grave falencia en materia de autonomía e independencia institucional.

Agregó que tanto las Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales como el nuevo Reglamento General de Protección de Datos de Europa son enfáticos en señalar que la Autoridad de Protección de Datos Personales o autoridad de control deben proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales, pero que para cumplir su rol deben ser ajenos, en el desempeño de sus funciones y en el ejercicio de sus poderes, a toda influencia externa, ya sea directa o indirecta, y no solicitarán ni admitirán ninguna instrucción.

Asimismo, aseveró que cada Estado debe garantizar que la autoridad de control disponga en todo momento de los recursos humanos, técnicos y financieros, así como de los locales y las infraestructuras necesarios para el cumplimiento efectivo de sus funciones y el ejercicio de sus poderes.

Acotó que la OCDE exige que la Autoridad de Protección de Datos personales debe contar con los recursos y la experiencia necesaria para el ejercicio de su función y la capacidad de demostrar que al tomar decisiones es objetiva e imparcial y tiene facultades para establecer las sanciones adecuadas.

Subrayó que todo lo anterior es incompatible con el diseño que el Ministerio de Hacienda propugna y en cuya defensa ha llegado a sostener que el Sistema de Alta Dirección Pública tiene importantes avances, omitiendo señalar que todavía están sujetos a remoción por el Presidente de la República cuando este asuma el cargo y que incluso la autoridad de control podrá ser despedida en cualquier momento, sin perjuicio

de las explicaciones que deban darse a la Dirección Nacional de Servicio Civil.

A modo conclusión señaló que los tiempos legislativos se agotan y si bien las particularidades del proyecto de protección de datos personales podrían discutirse al detalle, si queremos que vea la luz como ley de la República, bien podría sacrificarse alguna parte de esas discusiones a cambio de establecer que, además de los principios ya establecidos, la futura ley tendrá sanciones efectivas y una autoridad de control auténticamente independiente.

Consignó que solo con lo anterior ya tendríamos pavimentado el camino del reconocimiento nacional e internacional de Chile como un país con un nivel adecuado de protección de datos.

Concluyó señalando que si además a la autoridad de control se le dota de mecanismos directos o indirectos que posibiliten tener iniciativa en materia de ley dentro de su ámbito, la solución legislativa estaría completa y además, sería rápida y eficiente.

A continuación, **el Presidente de la Comisión, Honorable Senador señor Harboe,** ofreció la palabra **al Presidente de la Organización de Consumidores y Usuarios (ODECU), señor Stefan Larenas.**

El señor Larenas comenzó intervención señalando que la legislación vigente tenía originalmente por objeto contribuir a disminuir el riesgo país, al asociarse el tratamiento de los datos con un instrumento orientado al orden público económico. Por lo tanto, más que implementar un sistema de protección de datos personales lo que hizo, principalmente, fue regular el uso del dato económico.

Destacó que el resultado ha sido la instauración de un marco jurídico altamente permisivo, débil en cuanto a las posibilidades de control que pueden realizar tanto los titulares de datos como terceros y limitado en cuanto a la posibilidad de aplicar sanciones a las infracciones a los deberes que la ley establece.

Añadió que la mayor parte de la información personal, sensible o íntima, circula libremente por el mercado. Una empresa puede acceder a bases de datos de números celulares; a bajo precio se venden millones de cuentas de correo electrónico; las empresas de telecomunicaciones, comercios, bancos multitiendas y aerolíneas intercambian o adquieren periódicamente millones de datos personales.

En cuanto a las iniciativas en estudio, precisó que se busca incorporar la tendencia internacional de reconocer la protección de

datos como el derecho de las personas de controlar y proteger la información de la cual son titulares, de manera de lograr el resguardar los derechos fundamentales.

Recalcó que el ámbito de aplicación de la ley centra la protección en los datos personales, independientemente de si se encuentran o no en una base de datos, del soporte en que éstas se contengan o si el tratamiento de los mismos los realizan órganos del Estado, particulares o personas naturales. Señaló que intenta abarcar la mayor cantidad de operaciones posibles, como recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma.

En relación al consentimiento, sostuvo que el tratamiento de los datos personales solo se puede efectuar cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello. Asimismo se consagran excepciones, donde no se requiere autorización del titular cuando lo realicen personas jurídicas privadas para el uso exclusivo suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquello.

Hizo presente que se busca terminar con la práctica de revelar los datos relativos a obligaciones de carácter económico, financiero, bancario. Éstos han sido utilizados para negarles trabajo a las personas.

Respecto a la legitimidad de los datos, expresó que solo se pueden tratar los datos personales cuando el titular de los mismos consienta o medie una excepción legal. Igualmente, la finalidad consiste en que el tratamiento de datos debe limitarse a finalidades determinadas, explícitas y legítimas. En la proporcionalidad, el tratamiento de los datos debe limitarse a aquellos que resulten adecuados, relevantes y no excesivos en relación con la finalidad para la que se recolectaron. En la calidad, el responsable del tratamiento debe asegurar que los datos que trata son exactos, actuales y completos.

En relación a la transparencia, remarcó que el responsable del tratamiento deber tener políticas claras, legibles y en castellano sobre las operaciones de tratamiento de datos que realiza. En la responsabilidad, el responsable del tratamiento debe adoptar las medidas que permitan asegurar que cumple con los principios y normas sobre tratamiento de datos y contar con los medios que le permitan demostrar a los titulares de datos y a las autoridades que ello es así. Subrayó que en el ámbito de la seguridad, se deben adoptar medidas para evitar que el tratamiento de datos cause daños.

Añadió que la iniciativa del Ejecutivo garantiza los derechos de acceso, rectificación, cancelación, oposición y a la impugnación de valoraciones personales. Destacó que el derecho a la rectificación, para el consumidor común, ha sido casi inaccesible.

Agregó que en relación al derecho a la impugnación de valoraciones personales, se busca que no se adopten decisiones en contra de las personas basadas únicamente en el tratamiento de datos personales, de manera de minimizar las estigmatizaciones y discriminaciones fundadas en información que puede adolecer de problemas de calidad.

Luego, afirmó que el proyecto también cautela los derechos de las niñas y niños y les confiere legitimidad a partir de los 14 años. Recordó que si es menor se requiere el consentimiento de los padres.

Indicó que el proyecto del Ejecutivo crea la autoridad de protección de datos, bajo la fórmula de una corporación autónoma de derecho público, con personalidad jurídica y patrimonio propio.

Precisó que 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 el proyecto de 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.

Asimismo, recordó que la iniciativa del Ejecutivo considera infracciones leves, graves y muy graves, dependiendo del grado de afectación o amenaza de los derechos fundamentales de los titulares de datos.

Añadió que las sanciones que se consideran para cada tipo de infracción son de multas, sin embargo para infracciones calificadas como graves o muy graves en que haya reincidencia es posible además inhabilitar la base de datos. La cuantía de las sanciones se gradúa atendidos ciertos criterios que da la ley (por ejemplo carácter continuado de la infracción, beneficio obtenido por el infractor, reincidencia, grado de intencionalidad, etc.).

Connotó que las sanciones son aplicadas por la autoridad de protección de datos, a través de un procedimiento en sede administrativa que garantiza el debido proceso.

Concluyó su intervención consignando que se establecen reglas para que los órganos del Estado puedan intercambiar

información de las personas de manera de prestar servicios integrados a los ciudadanos.

A continuación, **el Presidente de la Comisión, Honorable Senador señor Harboe,** ofreció la palabra **al asesor legal del *Retail* Financiero, señor Eduardo Escalona.**

El señor Escalona manifestó que la legislación sobre protección de datos personales es necesaria para el país.

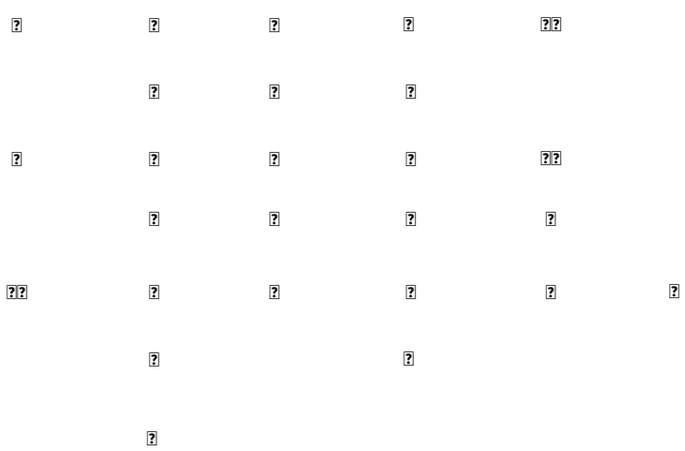
Agregó que su exposición la centraría en el análisis de los contenidos de ambos proyectos.

1.- Agencia de Protección de Datos Personales.

Señaló que es fundamental contar con la mencionada Agencia, y que ésta debe estar dotada de autonomía e independencia. Añadió que para lograr lo anterior, es importante que cuente con un gobierno corporativo.

Consignó que en el derecho comparado, dicha Agencia suele estar radicada en Comisiones. Por lo mismo, propuso que se podría seguir el modelo de la ley N° 21.000, que crea la Comisión para el Mercado Financiero.

Presentó el siguiente cuadro que explica las atribuciones razonables para una institución como la que se busca diseñar:



Luego, indicó que en la legislación nacional existen instituciones que desarrollan más de una atribución, sumando, por ejemplo, facultades interpretativas, normativas, fiscalizadoras y sancionadoras. Destacó que la mayoría de los organismos detallados suelen ser colegiados. Este tipo de organismo permite separar efectivamente el ejercicio correcto de las atribuciones.

Consideró fundamental la autonomía de la Agencia para poder obtener un ejercicio imparcial y un trato simétrico respecto de otros organismos que también tratan datos personales y dictan normas vinculadas a éstos. Precisó que ello no está cubierto en la iniciativa del Ejecutivo, y debe ser regulado.

2.- Coexistencia de Agencia de Protección de Datos y Sernac.

Recordó que en la ley N° 19.496, que establece normas sobre protección de los derechos de los consumidores, existen disposiciones que se refieren a temas de datos personales. Recalcó que ellas deben ser revisadas, porque tienen un componente propio de la relación de consumo y otro referido a datos personales.

Puntualizó que debe derogarse el artículo 28 B de la ley 19.496, sobre Protección de los Derechos de los Consumidores para resguardar la integridad y consistencia de la regulación de datos personales.

Aseveró que la revisión de eventuales cláusulas abusivas en relación a datos personales, debiera efectuarse exclusivamente por la Agencia de Protección de Datos Personales y no por el SERNAC, en aplicación del artículo 16 letra g) de la Ley 19.496. La mencionada disposición se refiere a aquellas cláusulas que dicen relación con la información del contrato y que deben ser interpretadas de buena fe.

Luego, se preguntó ¿quién revisa que esa cláusula cumpla con los estándares en la ley de protección de datos personales? Respondió que la Agencia debiera ser la llamada a cumplir esa función.

Remarcó que un aspecto relevante a tener en cuenta es que el Servicio Nacional del Consumidor tiene una cobertura nacional, situación que no ocurre con la Agencia quien, en sus inicios, tendrá presencia central.

Por lo tanto, sugirió que se debe lograr prontamente que la Agencia sea la única autoridad en esta materia y que tenga representación en cada una de las regiones.

3.- Consentimiento.

En este ámbito, destacó que en la definición del Mensaje se recoge que el consentimiento es una manifestación de voluntad libre, específica, inequívoca e informada. Agregó que sea inequívoca es clave respecto de múltiples relaciones contractuales. Ello permite dar fe cierta de que ha existido consentimiento.

Afirmó que no se puede circunscribir una legislación moderna exclusivamente a un consentimiento escrito. Recalcó que hay múltiples maneras de otorgar dicho consentimiento, sin que se produzca confusión alguna en términos de la voluntad.

Aseveró que en el proyecto del Ejecutivo se reconoce adecuadamente que existen diversos tipos de consentimientos, destacándose que la regla general para tratar datos personales es el consentimiento inequívoco.

Manifestó que el consentimiento inequívoco es clave en la aplicación sobreviniente de los contratos entre titulares de datos personales y los responsables de una base de datos.

Asimismo, señaló que es positivo que se reconozcan los diversos medios tecnológicos a través de los cuales se puede acreditar el consentimiento. Recomendó que el proyecto haga referencia a la ley N° 19.799 que regula la firma electrónica.

4.- Tratamiento de datos económicos, financieros y comerciales.

Compartió la idea de ampliar el alcance de los datos económicos, de manera que lo que los caracterice sea la finalidad de los mismos y no el documento o instrumento del que emanan.

Estimó que es tiempo de terminar con la cultura de la desconfianza en el uso de este tipo de datos personales. Ello implica no sustraer la información que emana de obligaciones de servicios públicos y

confiar en que el sistema de tutela de derechos que se busca incorporar es capaz de disuadir el mal uso y en el extremo sancionarlo.

5.- Derecho de cancelación.

Respecto de este punto, sostuvo que el mencionado derecho está cubierto por ambas iniciativas de ley. Recalcó que en el proyecto del Ejecutivo, específicamente en el artículo 7°, letra e) se consagra una excepción respecto del derecho de cancelación.

Ella dispone: “e) Cuando se requieran para la formulación, ejercicio o defensa de una reclamación formulada en el marco de esta ley.”.

Opinó que la excepción transcrita debe ampliarse a cualquier reclamación o juicio en que se afecte la relación entre el tratante y el titular de los datos. De lo contrario, el ejercicio del derecho de cancelación afecta el derecho a defensa de una de las partes.

Añadió que no se debiera prohibir al acreedor afectado a mantener y almacenar los datos de un deudor cuya relación contractual da cuenta de una deuda no pagada, ni aun cuando haya pasado 5 años desde que se hizo exigible.

6.- Sanciones accesorias.

En este ámbito, explicó que suspender el tratamiento de datos personales implica paralizar totalmente las actividades de múltiples empresas, por lo que es desproporcionado que la sanción accesoria sea más grave que la principal (multa).

Agregó que es indispensable establecer un catálogo de exenciones y atenuaciones de responsabilidad, pues también es desproporcionado castigar con este tipo de sanciones a sujetos por actuaciones de terceros.

7.- Modelo de prevención de infracciones.

En relación a estos modelos, destacó que es positivo que se promueva e incentive el cumplimiento de datos y se genere conciencia.

Enfatizó que hasta el momento, la única regulación de modelos de prevención se encuentra en la ley N° 20.393 de responsabilidad penal de las personas jurídicas.

Sugirió, por coherencia regulatoria, que así como se homologan las exigencias de los modelos de prevención, se le apliquen las mismas consecuencias jurídicas a quienes implementan dichos modelos, incluyéndose, por consiguiente, la posibilidad de configurar una exención de responsabilidad.

8.- Costos de la regulación e implementación gradual.

Señaló que la implementación de la nueva legislación conlleva inevitablemente mayores costos para todas las entidades que tratan datos personales. Connotó que se debe contar con una adecuada y oportuna difusión de sus contenidos.

Consideró que se debe efectuar una correcta capacitación de los funcionarios que se integrarán a la Agencia de Protección de Datos Personales.

Por lo anterior, sugirió que es indispensable una entrada en vigencia progresiva de la ley: 12 meses después de la puesta en marcha de la mencionada Agencia, y mantener el plazo de 5 años de adecuación del *stock* de las bases de datos actuales.

A continuación, **el Presidente de la Comisión, Honorable Senador señor Harboe** ofreció la palabra a **la abogada de FUCATEL, señora Lorena Donoso.**

La señora Donoso comenzó su presentación agradeciendo los esfuerzos desplegados por el Ejecutivo y por los Honorables Senadores que presentaron un proyecto de ley en esta materia.

Precisó que la presente discusión no significa la creación de nuevos derechos. Destacó que el artículo 5° de nuestra Carta Fundamental incorpora en nuestro país los tratados de derechos fundamentales suscritos por Chile. Agregó que los tratados de derechos humanos, en general, se refieren a la protección y resguardo de los derechos de las personas.

Constató que las leyes de protección de datos no buscan garantizar exclusivamente la privacidad, sino que el bloque general de derechos que se reconoce a las personas.

Aseveró que lo que genera más problema en la legislación vigente es la inexistencia de una autoridad de control y la ausencia de un régimen infraccional.

Agregó que se debe mejorar la autonomía e independencia de la Agencia de Protección de Datos, perfeccionar su gobierno corporativo, para los efectos de que sea útil. Sugirió que se establezcan reglas de inamovilidad del agente de protección de datos, si es que persistimos en una autoridad unipersonal.

Se preguntó por el nivel de autonomía y por el nivel de desarrollo que le vamos a reconocer a la autoridad encargada de la Agencia. Reiteró que su inamovilidad es fundamental.

Asimismo, manifestó que habiéndose previsto normas de tratamiento de datos personales en leyes específicas, en las que existen autoridades competentes para supervigilar el funcionamiento del sector de que se trate, tales como la Superintendencia de Salud, la Superintendencia de Pensiones, la Subsecretaría de Telecomunicaciones, por mencionar algunos, estos órganos en los hechos se han comportado como autoridad de control en materia de tratamiento de datos personales, impartiendo instrucciones, resolviendo reclamos, etc., lo que debe ser tenido a la vista a la hora de implementar esta nueva normativa.

Consignó que ambas iniciativas en estudio tienen una buena intención de adecuar nuestra legislación a los estándares actuales. Sin embargo, consideró que se debe tratar de mantener el carácter de ley paragua, y no inmiscuirse excesivamente en los temas específicos, porque ello nos puede llevar a entrampar la discusión.

Añadió que en materia de definiciones no es conveniente referirse a los datos biométricos ni a los genéticos, porque se pueden cometer errores, ya que son conceptos que provienen de una determinada ciencia o arte, que están condicionadas por estas últimas.

Constató que el alcance transnacional de esta normativa constituye una discusión inevitable, por cuanto en el mundo de servicios globalizados, no tenemos conocimiento de dónde éstos se prestan.

Remarcó que las distintas legislaciones han optado en radicar la protección al lugar donde se encuentra el sujeto titular de los datos personales. Afirmó que falta en la presente discusión, tomar lo positivo de ambas iniciativas y generar una propuesta intermedia en donde se resuelvan los problemas sustanciales de nuestra legislación, a saber, crear una autoridad de control que cumpla con los estándares internacionales; un régimen de infracciones y sanciones adecuado y establecer un mecanismo de tutela efectivo.

Luego, enfatizó que los modelos que propone el proyecto de ley del Ejecutivo se acercan bastante a establecer un tipo de tutela judicial efectiva con algunos antecedentes o aspectos que se pueden

mejorar, como por ejemplo, el de la dualidad de caminos tratándose de organismos públicos y privados.

En cuanto a la debida correspondencia y armonía entre el derecho a la libertad de expresión y la normativa sobre protección de datos, se manifestó de acuerdo en que hoy en día la prensa genera múltiples bases de datos que quedan a disposición *ad eternum* en los sistemas de información. Agregó que dichas bases de datos deben estar sujetas a los principios y normas de la ley de protección de datos.

Señaló que el eje central para comprender la normativa de protección de datos es que este tipo de leyes no protegen los datos, sino que resguardan a las personas que son titulares de esos datos respecto del tratamiento que hacen terceros de esa información. Recalcó que reconocen un principio fundamental que es la libre circulación de los datos.

Constató que éstos son necesarios. Los requieren las empresas y las instituciones públicas, y el mundo privado. Apuntó que el tema radica en cómo establecemos las reglas de tráfico de datos que garantizando la libre circulación de los mismos, no se vulneren los mecanismos de tutela judicial efectiva, para los efectos de evitar que ese tratamiento de datos termine en una resolución arbitraria.

Recalcó que las leyes de protección de datos buscan establecer sistemas de legitimidad en el tratamiento de datos para los efectos de que los titulares de éstos puedan ejercer adecuadamente sus derechos y no sean sujeto de discriminaciones arbitrarias.

Finalizó su intervención expresando que esta ley es indispensable, ya que constituye la única manera en que Chile entre en la economía de la información al nivel de los países donde queremos estar.

A continuación, **el Presidente de la Comisión, Honorable Senador señor Harboe** ofreció la palabra a los Honorables Senadores presentes.

En primer lugar, intervino **el Honorable Senador señor Larraín** quien manifestó que el tema central de la nueva normativa lo constituye la configuración de la Agencia de Protección de Datos. Preguntó si ésta si debe ser autónoma; unipersonal o colegiada.

Se mostró contrario a la propuesta formulada por el Ejecutivo respecto a la Agencia. Solicitó que los invitados a esta sesión se pronuncien al respecto.

Sostuvo que otra inquietud que tiene dice relación con el consentimiento. Consultó si éste se debe otorgar antes de que la información circule. Inquirió si debiese ser expreso o tácito.

Asimismo, señaló que las empresas que manejan bases de datos deberían consultar a los titulares de los datos. Recalcó que conciliar los principios referidos forma parte del desafío.

Añadió que en el proyecto hay un trato distinto respecto de los datos públicos y privados. Consignó que existen procedimientos y reclamaciones diferentes. Preguntó si ello se justificaba.

El Presidente de la Comisión, Honorable Senador señor Harboe, agradeció las presentaciones efectuadas. Explicó que cada una de ellas aportará diferentes miradas al desarrollo de esta nueva legislación.

Luego, explicó que se ha señalado la importancia de intentar sacar lo mejor de cada iniciativa. Aparte de ello también se deberá incorporar reflexiones que en esta sede se han planteado.

Advirtió que se debe poner en el centro de la discusión legislativa, la afectación de los derechos que hoy sufren los ciudadanos. Connotó que mediante una legislación equilibrada se podrá compatibilizar la libre circulación de datos y la debida protección de los mismos.

Destacó que el representante de la Asociación de Aseguradores de Chile A.G., expuso que puede ocurrir que la ley de protección de datos regule la actividad contractual, y se deje sin normar la etapa precontractual.

Asimismo, indicó que algunos plantearon que la institucionalidad propuesta por el Ejecutivo cumple los estándares de la OECD y que de aprobarse tal como está propuesta, Chile sería considerado un país seguro desde el punto de vista institucional. Otros plantean que lo anterior no es efectivo, puesto que hay otros compromisos internacionales que cumplir y de no acatarlos, nos veríamos privados de la categoría de país seguro.

Agregó que la representante de los Bibliotecarios manifestó una mirada distinta, porque, en general, estamos acostumbrados a circunscribir nuestro debate respecto de datos comerciales, sin embargo, es necesarios revisar aquellos relativos a temas literarios y a obras.

Finalmente estimó que es relevante la discusión que se ha planteado sobre el diferente trato que tienen los datos en el ámbito

público en relación a los del sector privado. Manifestó que se debe abrir la discusión de si esa diferencia se debe extender a las acciones de protección.

A continuación **el Honorable Senador, señor Harboe** ofreció la palabra a los expositores.

La señora Claudia Cuevas, representante del Colegio de Bibliotecarios de Chile, expresó que no parece conveniente que los datos inferidos sean transferibles (por ejemplo, historial de compras de Amazon, fichas médicas u otros), por cuanto, la generación de nuevos datos a partir de algoritmos de los datos compilados apuntan a predicciones que, no necesariamente, representan al titular de datos o que, en otros contextos ajenos a donde se produjeron, pueden inducir a error o, simplemente, a datos distintos resultado de interpretaciones inducidas.

Remarcó la relevancia de contar con profesionales idóneos en la Agencia de Protección de Datos Personales para el tratamiento y gestión de información, de tal forma, el almacenamiento y recuperación de datos (bibliotecarios, bibliotecólogos) responda a estándares y metodologías que permitan no solo la interoperabilidad y permanencia en el tiempo, sino también, compartir y enriquecer los datos, en particular, para aportar a la eficiencia de la administración de archivos, sobre todo, a nivel gubernamental.

Señalo que es interesante que las contrapartes de los consumidores y de los usuarios almacenen datos. Asimismo, consideró justo almacenar datos y registro de incumplimientos de las empresas.

A continuación, hizo uso de la palabra **la abogada de FUCATEL, señora Lorena Donoso**, quien sostuvo que, desde su percepción, han funcionado correctamente los modelos colegiados y unipersonales en materia de Agencias de Protección de Datos. Es decir, explicó que no es de la esencia que sea unipersonal o colegiado para que marche correctamente. Recalcó que la esencia la constituye la autonomía, la independencia y las atribuciones que tengan.

Afirmó que el Consejo para la Transparencia está en el ámbito de la transparencia, y no es fácil generar un balance respecto a dos derechos que básicamente son lo mismo, mirado desde dos ángulos.

Agregó que la composición que tiene actualmente el mencionado Consejo, hace difícil que éste sea un órgano de control, porque, por ejemplo, los consejeros no ejercen sus funciones en dicho organismo de manera exclusiva, y ello hace que sean representantes y directores de empresas que hacen tratamiento de datos personales, por lo tanto, quedarían inhibidos de dirigirle algún reproche a ellas.

Luego, y respecto al consentimiento, precisó que hoy en día, las legislaciones más avanzadas reconocen el consentimiento inequívoco como suficiente. Señaló que éste requiere de reglas de responsabilidad demostrada. Es decir, el proveedor que establece estos sistemas de consentimiento tiene que otorgar los medios de prueba necesarios para acreditar que la persona sabía lo que estaba consintiendo, y que fue libre al hacerlo.

En cuanto a las definiciones que formulan ambas iniciativas, aseveró que la Moción conceptualiza la disociación de datos erradamente, ya que ella corresponde a otra operación, que se denomina la seudonimización de datos. Ésta consiste en separar los datos de la identidad, pero además establezco reglas de custodia al protocolo con el cual se une el dato con la identidad, cuando así se requiera por distintas finalidades.

Recalcó que es peligroso establecer una definición de fuentes de acceso público que sea taxativa. Sugirió perfeccionar la definición del Mensaje, porque el hecho de que un registro esté abierto a la consulta de un titular o de un tercero no es suficiente para calificarlo como fuente de acceso público.

Finalmente, agregó que el registro de vehículos motorizados, o el de propiedad, no pueden ser fuente de acceso público, porque ellos se han establecido para los efectos de dar fe pública de ciertos hechos que son relevantes para la sociedad. Para ello se ha consagrado una institución garante, que se hará cargo de mantener la fiabilidad de ese registro.

En seguida, **el Presidente de la Organización de Consumidores y Usuarios, señor Stefan Larenas,** indicó que en cuanto al consentimiento se debe dar una discusión más profunda, sobre todo en la etapa precontractual. Enfatizó que el consentimiento debe ser inequívoco y explícito, éste no puede ser tácito.

Enseguida intervino **la Coordinadora de Mercado de Capitales del Ministerio de Hacienda, señora Bernardita Piedrabuena**, quien agradeció cada una de las presentaciones. Constató que su análisis permitirá mejorar el proyecto de ley de protección de datos personales.

En una sesión posterior, **el Presidente de la Comisión, Honorable Senador señor Harboe,** ofreció la palabra **al Director Nacional de Protección de Datos de Argentina, señor Eduardo Bertoni.**

El señor Bertoni agradeció la invitación a exponer ante la Comisión y la posibilidad de compartir con esta instancia el proceso que se está llevando a cabo en Argentina, en materia de protección de datos personales.

Explicó que la incorporación del *habeas data* al derecho constitucional se produjo en la reforma constitucional del año 1994. Agregó que dicha acción se refiere a la posibilidad que tienen las personas de conocer y pedir modificaciones de sus datos personales cuando éstos se encuentran en bases de datos. Precisó que al adquirir rango constitucional, se reguló, mediante ley, el mencionado derecho.

Sostuvo que la mencionada implementación se produjo recién en el año 2000. Agregó que transcurrieron muchos años de debate en la República Argentina, hasta llegar al texto actual de la ley de protección de datos personales.

Consignó que desde el comienzo del Gobierno del Presidente Macri, se propuso, entre otras cosas, la reinserción de Argentina en distintos foros internacionales, unido a la modernización de ciertos cuerpos legales, entre ellos el de protección de datos personales.

Relató que la reforma a la protección de datos se justifica por el impacto de las nuevas tecnologías, ya que ellas pueden llevar a provocar nuevas violaciones a la privacidad de los datos personales. Enfatizó que otra razón para actualizar la mencionada ley, está vinculada a un nuevo contexto normativo a nivel internacional.

Hizo presente que el Reglamento de Protección de Datos Personales que empezará a regir el próximo año en Europa dispone que el flujo de transferencias internacionales se podrá realizar únicamente con países que tengan legislación acorde a la legislación de dicho continente.

Aseveró que Argentina, desde el año 2003, ha sido considerado como un país adecuado para la Unión Europea, lo que ha facilitado el flujo de datos entre ellos. Afirmó que el proceso entrará en revisión a partir de la sanción de dicho Reglamento.

Señaló que el año 2016 comenzó en Argentina un proceso participativo en el marco de una plataforma establecida en el ámbito del Ministerio de Justicia y Derechos Humanos, conocida como Justicia 2020. A través de ella, el Ministro de Justicia y Derechos Humanos ha impulsado el debate en proyectos vinculados con reformas legislativas.

Agregó que la intención es que estas materias sean debatidas previa y extensamente antes de su ingreso al Parlamento.

Recalcó que Justicia 2020 constituye un espacio de diálogo institucional y ciudadano cuyo objetivo es la elaboración, implementación y evaluación de políticas para construir, junto a la sociedad, una justicia que genere resultados socialmente relevantes y permita la solución de los conflictos en forma rápida y confiable.

Aseveró que la mayoría de los actores involucrados, manifestaron la voluntad de que el Gobierno impulse una nueva ley de protección de datos personales. Recordó que se produjeron discusiones interesantes en cuanto a si era mejor hacer una nueva ley derogatoria de la anterior, o si se debía reformar parcialmente la legislación vigente. Consignó que la última opción correspondió a una posición minoritaria.

Reseñó que hubo cierto grado de cuestionamiento respecto a la necesidad de adaptar el consentimiento a los tiempos que corren en la era digital. La idea tenía que ver con la posibilidad de que se exigiera un consentimiento expreso en algunos casos muy específicos, como por ejemplo, tratamiento de datos sensibles, pero que en otros, éste pudiese tener algún grado de flexibilización.

Luego, connotó que otro de los temas que también se discutió fue el que dice relación con la transferencia internacional de datos. Sostuvo que la ley disponía que solo se permite hacer transferencia internacional de datos con países que tuvieran una legislación con una protección de datos similar a la Argentina. Añadió que el decreto reglamentario vino a morigerar la rigidez, incluyendo la posibilidad que aun cuando el otro país no tuviese una regulación adecuada o parecida a la de la mencionada Nación, se podría hacer igual la transferencia, siempre y cuando hubiese consentimiento. Como la ley nada decía al respecto, se generaron diversos problemas de interpretación.

Afirmó que una última materia que se discutió dice relación con la autoridad de aplicación y la independencia de la misma. Aseveró que la ley N° 25.326, del año 2000, tenía un diseño institucional muy adecuado, otorgando independencia a la mencionada autoridad. Sin embargo, al momento de promulgarse, el ex Presidente De La Rúa vetó dos incisos de un artículo, lo que provocó un daño a la independencia de dicha autoridad. Observó que el decreto reglamentario, un año después, tratando de enmendar el error, le otorgó a la autoridad de aplicación un formato que es el actual, creando la Dirección Nacional de Protección de Datos Personales. Agregó que ella se encuentra dentro del ámbito del Ministerio de Justicia.

Terminado el proceso de reflexión, se elaboró un primer borrador de un anteproyecto modificatorio de la ley N° 25.326, en

donde más allá de los temas aquí planteados, se agrega una cuestión fundamental, a saber, un cambio de enfoque que consiste en proteger los datos personales.

Añadió que también se crea la figura del delegado de protección de datos, como un funcionario de todas aquellas entidades privadas o públicas que tengan bases de datos, quien será el nexo entre la autoridad de aplicación y la empresa.

Asimismo, manifestó que tomando en consideración el derecho comparado, se advirtió que uno de los problemas que se plantea constantemente cuando estamos hablando de protección de datos personales y privacidad, es el que dice relación con el conflicto entre el ejercicio de la libertad de expresión y el acceso a la información pública.

Aseveró que el anteproyecto manda a hacer una suerte de interpretación donde no puedan dañarse otros derechos fundamentales en aras de la protección de datos personales. Connotó que la misma precaución se adopta respecto al derecho de supresión.

Observó que de esta manera están tratando de impulsar una legislación más moderna, que proteja los bienes y los derechos individuales de las personas, particularmente el derecho a la privacidad, y la protección de los datos personales.

Luego, recalcó que el gran desafío consiste en hacer este diseño institucional, legal, de manera que la mencionada protección no se constituya en una barrera que impida la innovación, la inversión y el avance de la tecnología.

Señaló que lo que se pretende es que mediante la iniciativa que se propone, Argentina se constituya en un polo tecnológico, en definitiva en un lugar atractivo para la tecnología que proteja derechos individuales.

Finalizó su exposición manifestando que la Dirección Nacional de Protección de Datos Personales ha venido liderando este proceso, con apoyo del señor Ministro de Justicia. Indicó que el anteproyecto se encuentra en proceso de revisión por el Ejecutivo previo a su ingreso al Parlamento.

A continuación, **el Presidente de la Comisión, Honorable Senador señor Harboe** ofreció la palabra **al Representante Adjunto de la Agencia Española de Protección de Datos, señor Jesús Rubí**.

El señor Rubí comenzó presentación señalando que la protección tradicional de la intimidad se articuló en torno al derecho al honor, a la privacidad, a la propia imagen, pero estos derechos resultaron insuficientes a partir del desarrollo de la informática. Expuso que con esta última surge un nuevo derecho que parte de la premisa de que habría un tratamiento generalizado de datos personales, pero sometiéndose éstos a una serie de reglas y de garantías.

Expresó que en el ámbito europeo hubo una primera oleada de disposiciones, a partir de una directiva del año 1995. Constató que actualmente en Europa cuentan con un Reglamento General de Protección de Datos que viene a actualizar la normativa, y a dar respuesta a desarrollos tecnológicos que no existían cuando se aprobó la anterior legislación. Consignó que el mencionado Reglamento realiza modificaciones relevantes en algunos aspectos, a saber, en el modelo de cumplimiento normativo; en el modelo de aplicación por parte de las autoridades y en la transferencia internacional de datos.

En cuanto al ámbito de aplicación de la norma, recalcó que vivimos en un entorno en el que infinidad de tratamientos de datos de los ciudadanos de un país son realizados por entidades que no se encuentran dentro de éste.

Aseveró que el mencionado Reglamento ha venido a establecer una norma de aplicación del derecho europeo a compañías que realizan tratamiento de datos fuera de la Unión Europea, y que son grandes prestadores de servicios de internet.

Mencionó que esos servicios pueden ir dirigidos a usuarios de *internet* en el territorio de un determinado Estado, o bien, que las mencionadas compañías se dediquen a monitorizar los hábitos de navegación en internet de los usuarios que residen dentro de dicha Unión.

Afirmó que de esta manera se da un sistema de protección global y se evita que exista un agujero negro en lo que se refiere a la protección de los servicios de dichas compañías.

Sostuvo que la tradición, por lo menos de la norma española, ha hecho conducir de manera excesivamente rigurosa la base jurídica para el tratamiento de datos en el consentimiento de las personas, ya sea inequívoco, o bien expreso o explícito en el caso de los datos sensibles.

Añadió que el Reglamento Europeo de Protección de Datos establece un sistema más flexible respecto a las bases jurídicas para el tratamiento de datos personales y parte de la premisa que siga existiendo este consentimiento o incluso los consentimientos reforzados.

Valoró del Mensaje del Ejecutivo de Chile que en caso de fallecimiento del titular de datos, los derechos que se reconocen puedan ser ejercidos por sus herederos.

Llamó la atención de la respuesta frente a las decisiones basadas exclusivamente en un tratamiento informático de la información sin intervención humana. Lo anterior, recordó, corresponde a algo que se ha generalizado en todos los entornos, especialmente en aquel que dice relación con la publicidad, que constituye la gran fuente de ingreso de los servicios gratuitos de internet, pero que se financian sobre la base de hacer una publicidad personalizada basada en los hábitos de navegación de los usuarios de la red.

Agregó que en el proyecto del Ejecutivo se recoge un derecho, en relación con las decisiones automatizadas, pero es un derecho que se vincula al ejercicio del derecho de oposición por parte de los titulares.

Luego, acotó que en el Reglamento Europeo se ha articulado de una manera distinta. En principio se reconoce el derecho a no ser objeto de una decisión automatizada sin intervención humana, y se reconocen derechos complementarios, tales como el derecho a conocer la lógica de ese tratamiento; a poder impugnar esa decisión y el derecho a obtener una explicación o una intervención humana que ratifique o modifique esa decisión.

Destacó que se ha incorporado también en el proyecto del Ejecutivo un derecho que está consagrado en el Reglamento mencionado, que es el derecho a la portabilidad de los datos personales. Constató que estamos ante un derecho muy relevante en un entorno en que existe gran cantidad de información y ella es facilitada voluntariamente por terceros y por los propios usuarios.

Hizo presente que el derecho de oposición se ha recogido de una manera causal. Agregó que se debe alegar un perjuicio para que opere este derecho. Afirmó que sería más flexible si en ciertos casos se exigiera la invocación de una causa, y en otros, como por ejemplo, en la realización del *marketing* directo, no sea necesario alegarla para dejar de recibir publicidad.

Señaló que es interesante la diferenciación de estándares de cumplimiento que permita adaptar la aplicación de esta norma a las distintas situaciones que puedan producirse en el ámbito de las administraciones públicas o en el caso de las Pymes. Sin embargo, consideró que en el proyecto del Ejecutivo se podría avanzar más respecto al modelo de cumplimiento.

Destacó que en la iniciativa antes mencionada se ha creado un registro de actividades de tratamiento en el que la autoridad de protección de datos debe certificar todas las políticas de privacidad de todos los responsables que hagan un tratamiento de datos personales. Enfatizó que para ello se debe dotar a la autoridad de una infraestructura de enorme capacitación y recursos financieros.

Manifestó que la solución viene dada por un modelo de cumplimiento proactivo donde son las propias entidades las que asumen la responsabilidad de mantener sus propios registros y asimismo deben mantenerlos a disposición de la autoridad de control. Añadió que en ese sentido se ha incorporado la figura del delegado de protección de datos. Ésta es una figura compleja que exige un nivel de capacitación muy importante.

Luego, en cuanto a los sistemas de autorregulación, sostuvo que éstos deben servir para adaptar a las características de un sector concreto las especificidades que tiene todo este sistema de garantías transversales. Además, indicó que los códigos de autorregulación en el Reglamento europeo, una vez que son supervisados, suponen una presunción de cumplimiento proactivo de la norma.

Precisó que hay un elemento añadido en los códigos de conducta de dicho Reglamento que consiste en incorporar sistemas de resolución extrajudicial o de mediación de las reclamaciones de los interesados. Planteó que ello lo deben hacer directamente ante las entidades infractoras.

Recordó que ha habido casos en el que determinadas reclamaciones, que podían tener una solución sencilla, al llegar al conocimiento de una autoridad de protección de datos se extienden, puesto que ella debe iniciar una investigación de los hechos y dar curso a un procedimiento administrativo.

Asimismo, en lo que se refiere al modelo de supervisión, subrayó que el Reglamento Europeo de Protección de Datos ha dado un salto fundamental, que no se encuentra en la iniciativa del Ejecutivo en discusión. El Reglamento posee sanciones que pueden ser demoledoras, pero al mismo tiempo tiene una serie de poderes correctivos que permiten modular y adaptarse a distintas situaciones de incumplimiento.

Igualmente, indicó que el referido Reglamento se ha flexibilizado para facilitar las transferencias internacionales de datos. Éste permite que haya una decisión de adecuación de países; de parte del territorio de unos países, o de sectores económicos de actividad concretos. Hizo presente que la decisión de adecuación constituye la fórmula más flexible que ha existido para facilitar la transferencia internacional de datos.

Precisó que Latinoamérica es uno de los principales importadores de datos. Agregó que esas transferencias tienen además la característica de ser transferencias internacionales de un exportador responsable de tratamiento a un importador en Latinoamérica encargado del tratamiento. Este último es un prestador de servicios que actúa conforme a las instrucciones que le facilita un tercero.

Constató que antes de la mencionada flexibilización, las cláusulas contractuales entre el exportador e importador tenían que ser autorizadas por la autoridad de protección de datos y generaba enormes rigideces.

Enfatizó que hay un artículo del Mensaje que señala que no se considerará que hay transferencia internacional cuando el importador de datos, en un tercer país, es un prestador de servicios, un encargado de tratamiento. Recalcó que hay que tener en cuenta que una de las principales prestaciones de servicios que se realizan en terceros países corresponde a los servicios de computación en la nube, y pretender que cualquier pequeño, mediano o gran operador sea el que va dar instrucciones a cualquier compañía multinacional que presta dichos servicios, no se aproxima a la realidad.

Finalizó su presentación señalando que las referidas comunicaciones de datos a terceros países tendrían que ser consideradas transferencias internacionales de datos e ir al mismo régimen de garantías. Lo anterior, argumentó, puede estar dado por cláusulas contractuales fijadas de manera homogénea por la autoridad de protección de datos.

A continuación, **el Presidente de la Comisión, Honorable Senador señor Harboe** ofreció la palabra a los Honorables Senadores presentes.

El Honorable Senador señor Larraín agradeció las exposiciones precedentes.

Manifestó que uno de los temas trascendentales de la iniciativa del Ejecutivo lo constituye la naturaleza de la Agencia que protege los datos personales.

Recalcó la importante labor que ha cumplido el Consejo para la Transparencia en el ámbito del acceso a la información pública. Agregó que el mencionado Consejo es autónomo y colegiado. Constató que éste ha logrado aplicar una legislación nueva, en un ámbito donde la cultura del secreto estaba instalada, haciendo transformaciones

muy profundas. Subrayó que ha sido capaz de supervisar y llevar adelante el proceso generando opinión, investigación y estudio.

Lo anterior, explicó, llama a pensar que la Agencia de Protección de Datos debe tener características similares. Preguntó si se logra el objetivo de la autonomía, mediante un órgano unipersonal que dependa del Ministerio de Hacienda, tal como lo propone el Mensaje.

Asimismo, se mostró partidario de contar con un organismo colegiado. Propuso que las labores de protección de datos personales recaigan en el Consejo para la Transparencia. Consultó a los invitados su opinión de lo planteado.

El Presidente de la Comisión, Honorable Senador señor Harboe inquirió a los invitados, si a su juicio, la consagración constitucional del derecho de protección de datos ha resultado un elemento positivo que ha significado un sometimiento del resto de la legislación y de las políticas públicas a entender, por ejemplo, el principio de autodeterminación informativa.

Preguntó cómo analizan la relación cada día más creciente entre la televigilancia y la protección de datos personales, particularmente en materias propias de la seguridad en espacios públicos.

En seguida, **el Presidente de la Comisión, Honorable Senador señor Harboe** ofreció la palabra **al Director Nacional de Protección de Datos de Argentina, señor Eduardo Bertoni**, quien sostuvo que la experiencia del Consejo para la Transparencia fue muy valiosa para los países de la región. Agregó que la constitución del mencionado Consejo constituyó un hito.

Expresó que es fundamental dotar de autonomía en el diseño a este tipo de órganos. Añadió que también a éstos se les debe entregar los instrumentos presupuestarios que requieren para funcionar.

Indicó que su país estaba atrasado en lo que respecta al acceso a la información pública. Aseveró que el Consejo para la Transparencia chileno colaboró en la implementación de una ley de acceso a la información pública en Argentina. Afirmó que en el mencionado cuerpo legal se creó una Agencia de Protección de Acceso a la Información Pública. Ella tiene carácter unipersonal. Aclaró que la discusión no se centró en el carácter colegiado o unipersonal del órgano.

Advirtió que la autonomía del órgano mencionado dice relación directa con la designación, la remoción y el manejo del presupuesto.

Hizo presente que la ley de acceso a la información pública creó una Agencia unipersonal en que la designación la realiza el Presidente de la República, a partir de un procedimiento reglado, transparente, de oposición de la sociedad civil. Subrayó que para la remoción necesita un dictamen vinculante de una Comisión Bicameral del Congreso Nacional.

Reiteró que lo detallado corresponde al diseño institucional que se le dio a la mencionada Agencia. Confirmó que ese mismo modelo se siguió en el anteproyecto de ley de Protección de Datos Personales. En este último se crea una Agencia con un Director que es designado por el Presidente de la República y para cuya remoción se requiere la aprobación del Parlamento. Añadió que la mencionada Agencia se crea como un órgano descentralizado dentro del ámbito del Ministerio de Justicia.

Consignó que crear un órgano completamente autónomo puede ocasionar un problema de índole constitucional, porque son órganos que habría que crearlos a nivel constitucional y para ello se debe reformar el mencionado cuerpo normativo.

En cuanto a la pregunta del Honorable Senador señor Larraín, respecto a si es conveniente que las funciones relacionadas con la transparencia y la protección de datos recaigan sobre el mismo órgano, apuntó que en el ámbito internacional no existe un único modelo. Agregó que en algunos países recae en una misma institución, y en otros se radica en dos órganos distintos.

Reconoció que ambas opciones tienen argumentos a favor y en contra. Estimó que la ventaja de tener un modelo en que ambos temas están juntos, tiene que ver con tratar de evitar un grado de litigiosidad, porque los conflictos se van a resolver dentro de la propia Agencia.

Connotó que si coexisten dos Agencias muy fuertes y separadas, se producirán conflictos entre ellas, y ello llevará a la judicialización de todas las decisiones.

En relación a la pregunta del Presidente de la Comisión, Honorable Senador señor Harboe, señaló que la consagración constitucional de los derechos siempre es positiva. Destacó que se produce una mayor conciencia de lo que significa el *habeas data* a partir de su inclusión en la Carta Fundamental.

Respecto a cómo hacemos para dar protección a datos personales y también converger en preservar la seguridad, aseveró que se debe trabajar para que ambas cuestiones tengan la relevancia que la

sociedad reclama y merecen. Acotó que no se puede menospreciar la privacidad de las personas en aras de la seguridad, pero cuando hablamos de los desafíos que representan la lucha contra la corrupción, el narcotráfico y el crimen organizado, debemos utilizar las herramientas que nos brinda la tecnología.

Finalmente, recalcó que está permitido recolectar datos masivamente, se puede obtener datos de las personas cuando tienen que ver con funciones del Estado vinculadas con la seguridad, pero hay que ser cuidadoso respecto de quiénes hacen el tratamiento y quiénes pueden acceder a ellos.

En seguida, **el Presidente de la Comisión, Honorable Senador señor Harboe,** ofreció la palabra **al Adjunto de la Agencia Española de Protección de Datos, señor Jesús Rubí**.

El señor Rubí manifestó que concordaba con lo expresado por el señor Bertoni respecto a que no hay un único modelo recomendable de autoridad que articule la protección de datos.

Agregó que en el artículo 8° de la Carta de Derechos Fundamentales de la Unión Europea se reconoce el derecho a la protección de datos y se señala que lo tutelará una autoridad independiente.

Adujo que al respecto, han consensuado, que lo fundamental de las distintas autoridades de protección de datos radica en la forma en que son nombradas; en su mandato; en el formato de garantías de los titulares del órgano; en que sus decisiones solo sean revisables ante la jurisdicción y que se le otorgue un hábito de control parlamentario directo del funcionamiento de la Autoridad.

Sostuvo que en el caso de España, el funcionamiento unipersonal ha generado una enorme eficiencia en relación con otros órganos colegiados de la Unión Europea, donde la toma de decisiones es bastante más compleja, porque la composición se articula en torno a la representación de uno u otro sector.

Señalo que en España, en materia de seguridad, la regla general en lo que respecta a la televigilancia es que el monopolio lo tengan las fuerzas y cuerpos de seguridad. Reconoció que en ocasiones se debe pedir autorización para poder instalar las cámaras a una Comisión de video-vigilancia que preside un magistrado.

Lo anterior no obsta a que la mencionada vigilancia se pueda admitir en el entorno privado. Consignó que existen sentencias del Tribunal de Justicia de la Unión Europea que han reconocido

el interés legítimo como una base adecuada para poder llevar a cabo la video-vigilancia.

Destacó que debe haber transparencia en la información, se debe garantizar la posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición, modulándolos a las peculiaridades de la video-vigilancia.

El Presidente de la Comisión, Honorable Senador señor Harboe agradeció la participación de los expositores. Asimismo alabó la labor que realiza el Consejo para la Transparencia al motivar esta discusión de alto nivel.

Estimó que Chile ha iniciado un camino sin retorno que tiene por objeto que se dicte una legislación que lleve a calificar al país como adecuado en materia de protección de datos.

En una sesión posterior, **el Presidente de la Comisión, Honorable Senador señor Harboe,** ofreció en primer lugar la palabra a los representantes de la Asociación de Telefonía Móvil (Atelmo).

En representación de la mencionada Asociación, hizo uso de la palabra **el Gerente de Relaciones Institucionales y Estratégicas, señor Cristián Sepúlveda** quien comenzó señalando que Chile se encuentra en deuda con respecto a la normativa de protección de datos. Agregó que si bien contamos con una ley relativa a la materia, ésta data del año 1999. Destacó que ella requiere ser actualizada para elevar los estándares de protección de los datos personales en Chile. Por ello es que Atelmo está de acuerdo en que la normativa en materia de datos personales se modernice y cumpla los estándares internacionales de la OCDE.

Asimismo, mostró su preocupación respecto a que la normativa que se dicte al efecto alcance el equilibrio natural que debe existir entre la protección de los datos personales y la utilización con fines comerciales o libre flujo de los mismos. Lo anterior cobra más importancia en la actualidad, ya que nos encontramos en la llamada economía digital.

Indicó que dicha economía está caracterizada por el intercambio de bienes y servicios realizado a través de plataformas tecnológicas y redes de telecomunicaciones, principalmente a través de internet. Aseveró que las interacciones entre las empresas, los proveedores y los consumidores se realizarán a distancia.

Sostuvo que la economía digital genera los siguientes efectos positivos:

1.- Reduce las barreras de entrada, de cambio y de salida.

2.- Eficiencia en la asignación de los recursos.

3.- Posibilita la creación de más y nuevos negocios.

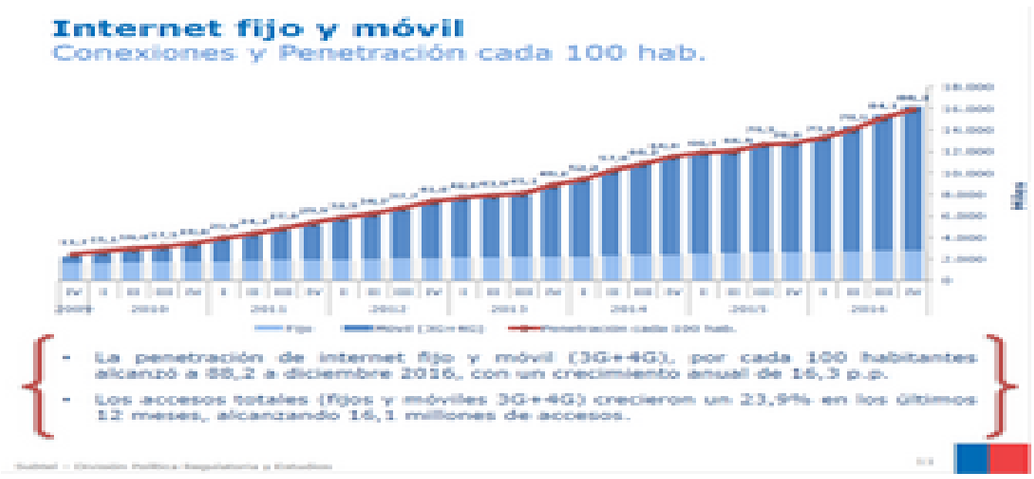
4.- Genera innovación.

5.- Provoca mayor competencia entre los oferentes.

6.- Aumenta la satisfacción de los consumidores.

Lo anterior, argumentó, ha generado que nos encontremos frente a un proceso de transformación digital.

Acompañó el siguiente cuadro que da cuenta de la conexión y penetración de internet.



Señaló que la economía digital requiere que no solo tengamos conexiones de internet, sino que se le dé a éste último una finalidad productiva que redunde en el beneficio de todos.

Manifestó que la economía digital y el tratamiento de gran cantidad de datos (*Big data*) es una gran oportunidad para la alianza público privada. Consignó que respecto al transporte público se puede monitorear cómo se desplazan las personas en determinados horarios; cuáles son los flujos; los horarios punta, etcétera. Lo mismo se puede lograr con las situaciones de catástrofe, ya que a través de la telefonía móvil se

puede, entre otras, definir el comportamiento de la población y se puede hacer un simulacro de tsunami.

En relación a los aspectos que pueden ser mejorados en la nueva normativa, enumeró los siguientes:

1.- Agencia de Protección de Datos.

Precisó que no es una agencia independiente, e irremediablemente estará sometida al ciclo político. Criticó su carácter unipersonal. Afirmó que países como Estados Unidos de Norteamérica, Francia, Alemania y México han optado por órganos colegiados.

Consideró que se requiere de un órgano colegiado que se haga cargo de las siguientes tareas:

- Dictar instrucciones y normas generales obligatorias.

- Interpretar normas legales

- Fiscalizar

- Requerir información

- Resolver Reclamos

- Sancionar. Régimen infraccional con multas relativamente altas y posibilidad de suspender el tratamiento de datos (art 42). Suspensión en casos calificados de transferencias internacionales (Art. 29).

- Exclusividad en la certificación y supervisar modelos de prevención.

- Determinación de si un determinado Estado cumple los estándares para transferencia internacional de datos.

Esta excesiva concentración de funciones pueden afectar los principios de imparcialidad y del debido proceso.

2.- Facultades que ejercidas en forma arbitraria podrían paralizar toda la actividad de un proveedor y afectar a millones de usuarios.

Destacó que el artículo 42 del proyecto del Ejecutivo dispone que la Agencia de Protección de Datos podrá suspender

las operaciones de tratamiento de datos hasta por un término de 30 días. Si no se da cumplimiento a dicho plazo puede aumentar por 30 días más, hasta completar seis meses. Posteriormente hasta la suspensión total.

Constató que en ese caso una empresa de telecomunicaciones podría verse expuesta a suspender sus servicios a sus 9 millones de clientes por 30 días. Recalcó que constituye una sanción desproporcionada en relación a sus efectos en una industria masiva como las telecomunicaciones.

3.- Restricciones del proyecto:

En este ámbito, destacó: a) la oferta de bienes y servicios en que existe una relación contractual preestablecida, o b) para comunicaciones publicitarias o de marketing ("*Opt in*" en vez de "*Opt out"*).

Consignó que dado que en el artículo 13 se elimina la excepción al consentimiento expreso para envío de comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios, dicha actividad requeriría ahora del consentimiento del titular de los datos.

Agregó que al exigir el consentimiento de los titulares, el Mensaje cambia el sistema actual "*Opt out*" por el sistema "*Opt in*" en el cual se requiere consentimiento (expreso, previo, libre, específico e informado) del titular de datos para el envío de dichas comunicaciones comerciales (*marketing* directo), luego, afirmó que no resulta lógico que el proveedor, que ya tiene una relación preestablecida, no pueda ofrecer bienes o servicios adicionales a aquéllos que ya ofrece a un determinado consumidor. Tampoco resulta razonable que un proveedor no pueda enviar comunicaciones comerciales o publicitarias de sus intereses específicos a un usuario. En todo caso, el usuario siempre debe poder dejar sin efecto el envío (*Opt out*). Finalmente, también genera una desventaja en el comercio nacional versus el comercio de empresas extranjeras.

Aseveró que la tendencia actual está dada por el *Marketing Analytics-Mobile Marketing*. Ellos están dirigidos a los intereses personalizados de los individuos.

Lo anterior producirá los siguientes beneficios:

a.- Se evita el *spam* no deseado;

b.- Mejora eficiencia a través de personalización de los mensajes;

c.- Asignación más eficiente de los recursos para ambas partes, y

d.- Mayor satisfacción de los usuarios.

4.- Cargas Desproporcionadas Para Responsables de Bases de Datos.

Manifestó que el proyecto se encuentra inclinado hacia una excesiva regulación de los datos personales y numerosas cargas responsables de bases de datos, que en la práctica transformará en muy costoso para las empresas el uso legítimo de los datos personales. En su estado actual, el proyecto podría afectar la libre circulación de los datos personales y, en consecuencia, disminuir o perder con ello la mejor asignación del valor económico y social de las tecnologías de la información en uso de los datos.

Añadió que incluso el Reglamento Europeo de Protección de Datos, considerado uno de los más estrictos en la materia, establece en su artículo 1°, que: “La libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta del tratamiento de datos personales”. Se parte de la base de que el objeto de la norma es el equilibrio entre la libre circulación de los datos y la protección de los mismos.

A continuación, mencionó algunos ejemplos de cargas desproporcionadas en el actual proyecto de ley:

- Art. 10.- Implementar mecanismos y herramientas tecnológicas para que el titular ejerza sus derechos en forma expedita, ágil y eficaz.

- Art. 14.- Obligaciones del responsable de datos. Letra a) Acreditar, cuando le sea requerido, los antecedentes que acrediten la licitud del tratamiento de datos que realiza.

- Art. 14 quáter. El responsable de datos debe adoptar las medidas necesarias para resguardar el cumplimiento del principio de seguridad establecido en esta ley considerando el estado actual de la técnica y los costos de aplicación. Se deberá tener en consideración la naturaleza de los datos y la probabilidad de los riesgos.

- Art. 14 quinquies.- El responsable debe reportar las vulneraciones a las medidas de seguridad, registrar estas comunicaciones, describiendo la naturaleza de estas vulneraciones, sus efectos, las categorías de datos y el número aproximado de titulares

afectados y las medidas adoptadas para gestionarlas y precaver incidentes futuros.

- Art. 15 bis.- Necesidad de autorización legal para mantener bancos de huellas digitales o de otros datos biométricos.

- Art. 2 Transitorio.- Da un plazo de 48 meses para ajustar todas las bases de datos a la nueva normativa, en tanto que los titulares pueden ejercer sus derechos a partir de la entrada en vigencia de la ley.

5.- Asimetría Regulatoria entre Empresas Domiciliadas en Chile y Aplicaciones Internacionales.

En esta materia, advirtió que la iniciativa del Ejecutivo no contempla la aplicación de la norma a quienes realicen tratamiento de datos personales de “chilenos” fuera del territorio nacional. Cualquier persona que trate datos de chilenos con fines comerciales, ya sea que su tratamiento se realice en Chile o fuera de Chile, debiera aplicársele la ley chilena.

Agregó que grandes conglomerados como *Google* y *Facebook*, los que han basado su desarrollo en los datos personales, y toman los datos de chilenos, no tendrán las restricciones de las empresas domiciliadas en Chile.

Indicó que se produce una grave asimetría frente al tratamiento de datos de chilenos, entre las empresas domiciliadas en el país y sometidas a la ley, respecto de aquellas no domiciliadas en Chile, que no se encontrarían reguladas. Lo anterior ocasiona inevitablemente la distorsión de la competencia.

Constató que una solución a este asunto, viene dada porque todo aquel que realice tratamiento de datos personales de “chilenos”, ya sea con fines comerciales o de perfilamiento, debe designar un domicilio, así como un responsable del tratamiento de datos en Chile.

Agregó que los riesgos en caso de no ajustarse la norma, son los siguientes:

- Fuga de capitales (innovación, *marketing*, servicios) hacia países con otros estándares más bajos, con una regulación más liviana en la protección de datos.

- Distorsiona la competencia. Regulación asimétrica para un mismo servicio o actividad, e

- Ineficacia de la ley. Dado que *Internet* es aterritorial, las empresas podrán realizar el tratamiento de datos personales de chilenos desde países con un estándar mínimo de protección de datos.

Sostuvo que como asociación gremial, ATELMO apoya la modernización y actualización de la legislación de protección de datos personales a los estándares OCDE, así como el otorgamiento de herramientas para que las personas puedan controlar la utilización de sus datos. Sin embargo, recalcó que no debemos olvidar que la economía digital es una realidad global que llegó para quedarse.

Añadió que Chile, como país en vías de desarrollo, es clave que aproveche la mencionada economía y absorba las eficiencias y beneficios que ésta genera, en especial en beneficio de los consumidores y usuarios de estos servicios, quienes buscan opciones cada vez más veloces, eficientes y a precios competitivos.

Finalizó su presentación señalando que es fundamental que esta regulación conserve este equilibrio entre la protección del dato personal y el libre flujo de los mismos.

A continuación, **el Presidente de la Comisión, Honorable Senador señor Harboe**, ofreció la palabra **al Consejero y Presidente del Comité de Innovación de la Sociedad de Fomento Fabril, señor Raúl Ciudad**, quien agradeció la posibilidad de presentar ante la Comisión las apreciaciones de la Sociedad de Fomento Fabril respecto a las iniciativas en discusión.

Manifestó que se requiere una legislación moderna para el tratamiento de los datos.

Expuso que la legislación vigente se encuentra desactualizada en materia de estándares de seguridad para los ciudadanos y no contiene reglas claras que permita el desarrollo del mercado del “*Big data*” en consonancia con los demás bienes jurídicos y derechos involucrados.

Expresó que la iniciativa del Ejecutivo mantiene inalterable la regulación de la información económica (Dicom), la que se deja aparte de esta reforma, lo que es correcto.

Agregó que el Mensaje deja amplios espacios al uso de información por parte del gobierno y sus reparticiones, sin que exista una protección de los derechos de los ciudadanos simétrica a la que se exige cuando ese manejo lo hacen las empresas.

Enseguida, se abocó a realizar observaciones específicas al proyecto de ley de Ejecutivo:

1.- Afectación de la libertad de expresión.

Sostuvo que la ley debe reconocer que la protección de datos personales debe respetar las garantías constitucionales de libertad de expresión y libertad de informar de toda la sociedad, y no únicamente las de los medios de comunicación social.

Propuso eliminar la referencia a “los medios de comunicación social”, de manera de hacerla extensible a cualquier persona que ejerza dicha garantía.

2.- Consentimiento libre.

Hizo presente que la exigencia que indica que el consentimiento otorgado por el titular debe ser libre, no contribuye a perfilar el tipo de consentimiento que se requiere.

Apuntó que no se proporciona el nivel de detalle que se le otorga a este concepto y puede resultar redundante, tomando en consideración que, por regla general, se entiende que el consentimiento que otorga una persona debe ser libre, es decir, exento de vicios del consentimiento, debiendo probar lo contrario quien alega su ocurrencia.

Es más, destacó que esta exigencia puede generar discusiones y problemas en la aplicación de esta norma.

3.- Principio de seguridad.

En este ámbito, sugirió que en el artículo 3° del proyecto del Ejecutivo se agregue el concepto de razonabilidad respecto a los niveles adecuados de seguridad que se deben adoptar en el tratamiento de datos personales, de tal manera que se tome en consideración la naturaleza del dato objeto de tratamiento.

Asimismo, propuso eliminar la referencia al “daño accidental”, debido a que conforme la definición doctrinal del mismo, este tipo de daño puede equipararse al caso fortuito, lo cual es contradictorio a las reglas generales que rigen en materia de responsabilidad en nuestro ordenamiento jurídico.

4.- Derecho de oposición.

Indicó que en la regulación del derecho de oposición que contiene el Mensaje, no se indica cual es la consecuencia práctica de la oposición, es decir, si ello supone el bloqueo de los datos, en cuyo caso entenderemos que el responsable podrá seguir almacenando esos

datos, o bien la supresión de los mismos, en cuyo caso se trataría del mismo efecto práctico del derecho de cancelación.

Se mostró partidario de limitar la causal indicada en la letra a) del artículo 8, relativa a la afectación de derechos y libertades fundamentales, ya que al ser tan amplia puede llevar a que finalmente el titular de datos personales siempre tenga derecho a oponerse al tratamiento, sin que exista necesidad de esgrimir otra causa.

Explicó, que atendida la regulación antes señalada, el responsable de datos debe asumir que el titular siempre podrá oponerse y que, por tanto, no existirá certeza de poder contar con dichos datos de forma sostenida en el tiempo.

Recomendó incorporar todos aquellos casos en los cuales no proceda el ejercicio del derecho de oposición, siguiendo el formato que se utiliza para el derecho de cancelación, y establecer que no podrá hacerse uso de este derecho de oposición, en el evento que, el tratamiento sea necesario para ejercer el derecho a que se refiere el artículo 19 N° 12 de la Constitución Política de la República.

5.- Intermediario tecnológico.

En este ámbito, sugirió reconocer y definir el rol del “intermediario tecnológico”, quien es aquel que pone a disposición un servicio tecnológico que involucra tratamiento de datos recopilados por terceros.

Apuntó que debe establecerse cuál es su responsabilidad respecto al uso de sus sistemas, atendido el hecho que el no fiscaliza el contenido de los datos ni toma decisiones respecto al uso de los mismos.

6.- Transmisión de datos personales.

De lo dispuesto en el artículo 29 del proyecto de ley de Ejecutivo, se desprende que la transmisión de datos personales, y en consecuencia los servicios en la “nube”, no estarán sujetos al régimen especial de transferencia internacional, aun cuando el tercero que efectué el tratamiento se encuentre sujeto a la legislación de otro país.

Atendido lo anterior, advirtió que es contradictorio el hecho que respecto a las transmisiones internacionales de datos, la Agencia pueda adoptar medidas conservativas, y suspender, en casos calificados, el envío de datos, ya que ellos estarían expresamente excluidos del régimen aplicable a la transferencia de datos.

Agregó que adoptar este tipo de regulación, genera un escenario de incertidumbre, afectando la libre circulación de la información, entorpeciendo el futuro desarrollo de tratamiento lícito de los datos personales y modificando el mercado digital en estas materias.

Asimismo, recomendó las siguientes medidas:

- Excluir expresamente los servicios en la nube de la transferencia internacional de datos, por cuanto se trata de una transmisión de datos.

- Eliminar expresamente del inciso final del artículo 29 del Mensaje, la transmisión de datos y los servicios en la nube, de las facultades normativas o medidas conservativas que se le entregan a la Agencia.

7.- Multas

Respecto a los criterios para la determinación de las multas sostuvo que no es adecuado incluir dentro de los factores de cálculo la distinción del tipo de persona que comete la infracción, es decir, si se trata de persona natural o jurídica o si se trata de una entidad con o sin fines de lucro.

Asimismo, propuso tomar en consideración para tales efectos, como lo señalan otras legislaciones, la capacidad económica del infractor.

8.- Principio de coordinación

En relación a este punto, argumentó que si bien la iniciativa contempla expresamente este principio, surge la duda de cómo, en la práctica, se coordinarán la Agencia con la Contraloría General de la República, quien es la llamada a sancionar a los órganos públicos, y la Agencia y la Contraloría con el Consejo para la Transparencia, quien deberá velar por el adecuado cumplimiento de la ley N° 19.628, en los ámbitos de la transparencia en la función pública y el acceso a la información.

En cuanto a la comparación entre el sector privado y los órganos públicos presentó los siguientes cuadros:

Sector privado v/s órganos públicos

Aspectos a comparar	Sector Privado	Sector Público
Consentimiento previo	Si	No
Derechos del titular	Acceso Rectificación Cancelación y oposición Portabilidad de los datos	Acceso Rectificación Cancelación y oposición (ejercicio restringido) No aplicaría

Sector privado v/s órganos públicos

Aspectos a comparar	Sector Privado	Sector Público
Cesión de datos personales	La cesión de datos personales requiere el consentimiento previo de su titular, salvo las excepciones legales	Listado de casos cuando es procedente la cesión de datos personales (numerus clausus)
Reclamación administrativa	Reclamación ante la Agencia Recurso de reposición	No existe procedimiento especial
Reclamación judicial	Recurso de ilegalidad ante la Corte de Apelaciones, quien **deberá** requerir informe a la Agencia con el objeto de establecer si hubo infracción	Recurso de ilegalidad ante Corte de Apelaciones, quien **podrá** requerir informe a la Agencia con el objeto de establecer si hubo infracción

Sector privado v/s órganos públicos

Aspectos a comparar	Sector Privado	Sector Público
Responsabilidad administrativa	Agencia impone sanciones Multas: amonestación escrita y multas de 1 a 5.000 UTM Se establece un procedimiento sancionatorio especial Respecto de la resolución sancionatoria procede recurso de ilegalidad ante la Corte de Apelaciones	Agencia determina las infracciones y las CGR impone las sanciones Multas: Regla general: 20% a 50% de la remuneración mensual, y multas duplicadas y suspensión del cargo hasta por 30 días, en caso de infracción reiterada En caso de datos sensibles, la multa será del 50% de la remuneración y suspensión hasta 30 días
Responsabilidad civil	Daño patrimonial y moral causado al titular	No se aplicaría

Sector privado v/s órganos públicos

Aspectos a comparar	Sector Privado	Sector Público
Tratamiento de datos por un tercero	Régimen contemplado en el artículo 15 bis del Mensaje	No se aplicaría
Certificación modelo de prevención	Implica atenuante de responsabilidad administrativa	No se aplicaría
Publicidad de las sanciones	Registro Nacional de Cumplimiento y Sanciones que lleva la Agencia	Sitio web de la Agencia y del respectivo órgano público

Finalizó su presentación señalando que en relación al principio de coordinación de los órganos del Estado, de acuerdo al artículo 21 del proyecto del Ejecutivo, estas entidades deben propender a un alto grado de interoperabilidad y coherencia de modo de evitar contradicciones en la información almacenada y reiteración de requerimientos de información o documentos a los titulares de datos. Sin

perjuicio de que la iniciativa contemple expresamente el principio, afirmó que surge la duda de cómo en la práctica se coordinará la Agencia con la Contraloría, quien es la llamada a sancionar a los órganos públicos.

A continuación, **el Presidente de la Comisión, Honorable Senador señor Harboe**, ofreció la palabra **al socio de Destácame, señor Augusto Ruiz Tagle**.

Al iniciar su presentación indicó que Destácame constituye una plataforma gratuita que ayuda a las personas a acceder a créditos usando información alternativa. Agregó que la clave consiste en que se permite que las personas conozcan su situación financiera y luego, a través de información, puedan acceder a mejores productos financieros. Asimismo ayudan a que éstas paguen y se reinserten en el sistema financiero.

Constató que la mitad de la población de Latinoamérica está excluida del mencionado sistema. Asimismo, manifestó que con el consentimiento de los usuarios de Destácame se puede acceder a distintas fuentes de información que no están disponibles en el mencionado sistema. Por lo tanto, argumentó, se genera un mayor conocimiento para evaluar el riesgo de las personas. Recalcó que ellas se adueñan de la información.

Sostuvo que respecto a los lineamientos bases para la regulación de datos personales, aplicados al sistema financiero, existen dos pilares principales, a saber:

1.- Incentivar el mayor acceso y mayor uso de fuentes de información.

Explicó que en este ámbito existen cuatro dimensiones.

a.- El acceso.

Respecto a éste, precisó que se trata de empoderar a las personas para que se adueñen de la información como un gran activo. Añadió que se debe contar con validación online. Hizo presente que el mundo está cambiando y la regulación se debe preocupar de mejorar y detallar cuáles son las condiciones para poder acceder a la información personal mediante mecanismos online, por un tema de reducción de costos y de facilidad de acceso a productos y servicios.

Constató que se deben generar mecanismos básicos para asegurar el acceso, partiendo por el Estado.

b.- Usos.

Manifestó que se debe incentivar la diversidad de uso de diferentes fuentes de datos y nuevos modelos de negocios. Recalcó que se deben generar incentivos de largo plazo.

c.- Aplicación de la ley.

Señaló que se debe asegurar el acceso a la información y mejorar herramientas y aumentar recursos para que la ley se aplique. Agregó que la Agencia de Protección de Datos viene a mejorar sustancialmente este aspecto.

d.- Adaptabilidad.

Precisó que busca ampliar la aplicación de la ley a las micro, pequeñas y medianas empresas que en general no son consideradas. Enfatizó que los datos que ellas manejan son normalmente ignorados.

2.- Permitir pruebas de nuevos modelos de negocios. (*Sand Boxes Regulatorios*)

Sobre este aspecto sostuvo que las nuevas tecnologías se deben probar rápido para demostrar su valor. Detalló que ellas tienen un área de acción definida con el objeto de minimizar el riesgo de prueba.

Añadió que las instituciones pueden accionar propuestas con menor burocracia interna. Aseveró que se busca generar un cambio cultural en un ambiente que ha priorizado la certeza, con una baja tolerancia al error.

Luego, en relación a los proyectos en estudio realizó las siguientes observaciones:

En primer lugar, propuso mejorar algunas definiciones para dar poder a los titulares de los datos. Remarcó que el proyecto del Ejecutivo no explicita quién tiene la propiedad de los datos.

Puntualizó que se deben identificar casos de uso y aplicación de la ley. Explicó que los criterios deben ser distintos, atendido el tamaño de las bases de datos.

Asimismo, hizo presente que se debiera precisar los términos “ágil y eficaz” y “frecuencia” para la entrega de datos. Se

preguntó, en términos de acceso a la información, ¿cuándo se puede cobrar por una frecuencia mayor y cuál es el máximo?

Igualmente, cuestionó, en relación a las obligaciones del administrador de datos, cómo se facilita el flujo de la información cuando se trata de un titular de datos que quiere transmitirlos a una tercera persona.

Señaló que no se define cómo tiene que estar representado el titular de los datos frente al administrador.

Requirió mayor detalle en definiciones para casos de uso *online*. Lo anterior, argumentó, es clave para este tipo de regulación.

Por otra parte, advirtió que se debe contar con distintos niveles de validación de identidad según sensibilidad de la información. Aseveró que la Agencia es la llamada a hacer esta labor.

Manifestó que ciertos temas se deben revisar aplicando estándares internacionales, como por ejemplo, el flujo fronterizo de datos; el almacenamiento y tratamiento de datos en organismos públicos, y la extensión de aplicación a datos financieros (incluir SBIF y otras superintendencias).

Recalcó que la Agencia de Protección de Datos es la llamada a establecer el estándar único entre organismos del Estado para poder acceder a fuentes de información. Sostuvo que debiera existir una coordinación entre la Agencia y el Consejo para la Transparencia.

Aseveró que Destácame tiene más de 300.000 usuarios en la plataforma que administra, quienes han opinado sobre este proyecto. A continuación, enumeró algunos de esos comentarios:

1.- “Mantener la reserva de datos en todo momento”;

2.- “Sugiero prohibir a los comercios el pedir el RUT de los clientes como requisito para compra”

3.- “Los datos personales son vendidos; prohibir esta práctica con multa equivalente a tres veces el valor de la venta”

4.- “Debería existir un registro único de datos donde se almacene la información de las personas, que pueda ser consultado por quien lo desee, pero con previa autorización de los afectados.”

Finalizó su presentación declarando que debiese existir una base de datos única para facilitar el acceso al ciudadano, sin que tenga que recurrir a los distintos organismos en busca de ella.

A continuación, **el Presidente de la Comisión, Honorable Senador señor Harboe,** ofreció la palabra a **la Gerente de Políticas Públicas de *Google*, Cono Sur, señora Eleonora Rabinovich,** quien agradeció a la Comisión la posibilidad de dar la visión de la empresa que representa en este tema tan importante.

Saludó la iniciativa del Congreso Nacional de discutir las reformas a la ley actual, ya que es importante que Chile cuente con un marco normativo moderno y actualizado de protección de datos personales.

Estimó que la regulación adecuada del tratamiento de datos personales; la protección de la privacidad en internet y la seguridad de la información personal de los usuarios son temas que *Google* toma con suma seriedad y se sitúan dentro de sus prioridades.

Comentó que la empresa en Chile cuenta con alrededor de sesenta empleados. Remarcó que *Google* escogió a Chile como sede del único centro de datos que la compañía tiene en América Latina.

Explicó que una de las razones por las cuales la empresa apostó por Chile, es porque el mencionado país ha estado a la vanguardia en temas de regulación de *internet*.

Sostuvo que la discusión sobre datos personales es una oportunidad histórica para que Chile marque tendencia de vanguardia en la región y en el mundo.

Luego, aseveró que el respeto a la protección de datos no es incompatible con la utilización de los datos al servicio de los usuarios para crear nuevos y mejores productos y servicios. Enfatizó que la privacidad constituye un esfuerzo permanente en dicha compañía y cientos de empleados dedican su tiempo a proyectos que están relacionados con ella.

Manifestó que hay cuatro pilares sobre los que la empresa basa sus medidas de privacidad y seguridad, a saber:

1.- Elección.

Proporcionan a los usuarios elecciones sobre su privacidad a lo largo de la vida de su cuenta en *Google*. Al comienzo, cuando

se crea la cuenta; durante el uso de ella y al final de la vida de la misma, ya sea por abandono o por cancelación.

2.- Transparencia.

En este ámbito señaló que ayudan a los usuarios a tomar buenas decisiones sobre su privacidad, haciendo fácil que puedan ver qué datos recoge la compañía para permitir la personalización y la publicidad.

3.- Control.

Explicó que la empresa entrega controles de privacidad robustos que aseguran que los usuarios tengan una experiencia con Google en sus propios términos.

4.- Seguridad.

Luego, afirmó que los datos de los usuarios son sagrados. Reconoció que la empresa realiza una gran inversión para que los datos de los usuarios sean accesibles para ellos.

Subrayó que sin seguridad no hay privacidad y tampoco hay elección sin control, ni control sin transparencia. Hizo presente que para hacer realidad los mencionados pilares ofrecen distintas herramientas a los usuarios.

En relación a los proyectos de ley en discusión, comentó que las oportunidades de desarrollo económico asociados a las tecnologías son las más importantes en la actualidad. Aseveró que en Chile la economía digital representa el 3% del PIB. Advirtió que ese indicador seguirá aumentando.

Agregó que la economía digital es una economía basada en datos. Manifestó que para capitalizar las oportunidades de desarrollo económico y social generadas por *internet*, se requieren políticas flexibles que hagan foco en la seguridad del flujo de datos, en lugar de limitar la innovación.

Seguidamente, consignó que existen distintos modelos de protección de datos personales. Añadió que el modelo europeo, representado por el Convenio 108 y los reglamentos generales de datos personales inspiraron gran parte de los proyectos de ley que se han presentado sobre esta materia.

Reseñó que el modelo de privacidad Apec es interregional e interesante. Señaló que también existen otros modelos híbridos, domésticos, como los de Canadá, México y Japón.

Como miembros de la OEA, recordó los principios de privacidad dictados que buscan equilibrar la protección de los datos personales con otros derechos, como por ejemplo, el de la libertad de expresión.

Expuso que las iniciativas en discusión dan pasos positivos cuando incorporan algunas de las mejores prácticas internacionales, como son, por ejemplo, la flexibilidad que se expresa en cuanto a los diferentes matices que se puede presentar con la figura del consentimiento o la inclusión de las prácticas de la responsabilidad demostrada.

En cuanto al alcance, se mostró partidaria de que se discuta o se revise el hecho de que en ambos proyectos se desvincula el alcance y ámbito de aplicación de los datos contenidos en bases de datos, entendidas éstas como el conjunto ordenado de datos personales en posesión de un responsable.

Agregó que en la redacción actual de los proyectos, se desprende que la ley sería aplicable a datos personales de manera genérica, amplia y abierta. Estimó que lo anterior puede generar incertidumbre en relación con determinar cuáles serían los sujetos obligados y el ámbito de aplicación de la norma. Recomendó introducir una definición de base de dato y conceptualizar al responsable como aquel que decide acerca del tratamiento de las bases de datos que obran en su poder.

En relación al ámbito territorial de aplicación de la ley, consideró que las prohibiciones de aplicación extraterritorial de la ley chilena podrían entrar en conflicto con los principios del derecho internacional y ello puede derivar en conflictos de leyes de muy difícil resolución y por otra parte que los responsables estén sujetos a distintas leyes. Afirmó que ello generaría incerteza jurídica en relación a cómo se van absolver los conflictos y por otra parte puede perjudicar el arribo de bienes y ofertas o servicios para los usuarios chilenos.

Sostuvo que la ley local no puede pretender ir más allá de las fronteras. Lo que sí puede implementar es una exportación de circulación transfronteriza de datos segura y bajo ciertos estándares interoperables y compatibles. Es decir, la ley local puede determinar cuáles son las reglas para la transferencia internacional.

Sobre el tema de bases del tratamiento, manifestó que es limitante que el consentimiento sea la única base legal del tratamiento y que no se incluya de manera expresa y clara a los intereses legítimos.

Destacó que en la era del *Big data* o del *internet* de las cosas, resulta imprescindible que las legislaciones se adapten a las nuevas realidades.

Añadió que los intereses legítimos constituyen una base legal tan imprescindible como el consentimiento y sugirió que se le incluya en el texto final. De esta manera, argumentó, el tratamiento de los mencionados intereses sería pionero en América latina y podría sentar un precedente de innovación en la región. Dijo que tratándose de un concepto novedoso, la ley podría incluir una lista no exhaustiva de supuestos que podrían considerarse como intereses legítimos.

En ese sentido, expresó que los considerandos 47, 48 y 49 del Reglamento Europeo ofrecen distintos supuestos de intereses legítimos, como por ejemplo, prevención del fraude; seguridad en las redes de infraestructuras, *marketing* directo, y administración de las bases de datos de clientes y empleados.

Destacó la necesidad de no limitar el alcance de dicha base legal a ciertas categorías de datos, como puede ser, por ejemplo, los datos accesibles al público. La ley de datos constituirá la base de la economía digital, por lo tanto, es importante pensar cuáles son todas las herramientas que podemos dar para que despegue la innovación en un mercado como el de Chile.

En relación con los datos sensibles, propuso introducir una lista cerrada de los supuestos en que los datos personales puedan considerarse sensibles, eliminando la posibilidad de que la lista pueda ampliarse hasta el infinito, ya que generaría incertidumbre.

Recalcó que la ley debe tener una definición clara de los actores. Llamó la atención respecto al rol que cumplen los intermediarios tecnológicos. Por una parte proveen servicios y plataformas en los que un usuario sube información, que puede o no ser personal, y el intermediario no lo sabe y tienen un equivalente en la vida *off line*.

Seguidamente hizo presente que es importante introducir la figura del intermediario tecnológico con su consiguiente limitación de responsabilidad. Agregó que ella responde a un concepto que ya existe en la normativa chilena, específicamente en la ley N° 17.336 de Propiedad Intelectual. Esto es así porque el proveedor de estos servicios, no conoce, ni debe conocer, el contenido de la información.

Precisó que otro tema que debe ser incluido en una ley de protección de datos, es el balance con otros derechos, en particular con el de la libertad de expresión.

Expresó que el derecho de cancelación debe ser cuidadosamente equilibrado con otros derechos. Enfatizó que debe clarificarse la excepción de libertad de expresión e interés público cuando se establece el ejercicio del derecho de cancelación.

Asimismo, consideró que en el proyecto del Ejecutivo, el derecho de oposición está concebido con gran amplitud, con lo cual un operador debería asumir que el titular siempre tendrá derecho a oponerse al tratamiento de datos. Agregó que el mencionado derecho se ejerce cuando la base legal no es el consentimiento, ya que este último, por definición es revocable. Advirtió que hace falta adecuarlo al principio de incorporación de los intereses legítimos.

Sostuvo que se deberían revisar algunas restricciones que están impuestas específicamente al sector de la publicidad. Estimó que la futura ley debiese mantenerse neutral, al margen de tecnologías y sectores, especialmente cuando se trata de establecer obligaciones, restricciones y prohibiciones. Por otra parte, señaló que se podrían generar estereotipos negativos que no tienen siempre una adecuada justificación y que pueden causar daños a una industria que puede ser legítima.

Destacó que la excepción del ejercicio del derecho a la libertad de expresión debe inspirar todo el procedimiento para el ejercicio de los derechos del titular. Consignó que Chile ya ha incorporado el estándar de notificación judicial, es decir, que solamente es el Poder Judicial quien puede determinar el balance de derechos y actuar en consecuencia para remover el contenido, presuntamente infractor en la ley N° 17.336, de Propiedad Intelectual. Opinó que dicho estándar no debería ser debilitado en la presente discusión. Esto se relaciona, explicó, con los procedimientos establecidos para la protección de los derechos de los titulares. Connotó que el adecuado balance de derechos solo puede ser realizado por un juez, de acuerdo también a los estándares del Sistema Interamericano de derechos humanos.

En relación a las transferencias internacionales de datos, aseveró que ello es de vital importancia en el marco de la economía digital. Subrayó que en la redacción actual del proyecto, la propuesta limita la posibilidad de las transferencias internacionales cuando medie el consentimiento o se trate de un país que ofrezca un nivel adecuado de protección. Es decir, la base sigue siendo el consentimiento y la adecuación y luego hay una serie de excepciones.

Se preguntó por el motivo de partir por la prohibición, cuando se puede permitir la adecuada transferencia, siempre y cuando se cumplan determinadas condiciones.

Mencionó que la adecuación no es el único sistema que se puede tomar en cuenta. Agregó que países como Singapur, México o Canadá adoptaron esquemas que permiten el libre flujo de datos y que sujetan las operaciones de procesamiento a revisiones ex post, por parte de las autoridades.

Concluyó su presentación afirmando que existen distintos instrumentos que pueden ser utilizados en esta materia.

A continuación, **el Presidente de la Comisión, Honorable Senador señor Harboe** ofreció la palabra **a la Directora del Instituto Nacional de Estadísticas, señora Ximena Clark**.

Al comenzar su presentación señaló que opinará sobre el proyecto de ley desde el punto de vista de la actividad estadística. Remarcó que esta última en Chile tiene un nivel de centralización no menor, en donde el INE es un ente importante y protagónico, pero no es el único que elabora estadísticas.

En cuanto a las características generales del proyecto, destacó lo siguiente:

1.- Se construye sobre el principio esencial en materia de protección de datos personales: “la libre circulación de datos en condiciones debidas”.

2.- Incorpora principios reconocidos en instrumentos internacionales (principios y lineamientos de ONU, OECD, UE) y en la legislación comparada.

3.- Presenta una adecuada explicitación de derechos y obligaciones para los responsables de las bases de datos y los respectivos titulares de datos.

4.- Se conceptualiza en su rol supletorio a las reglas especiales, tal como ocurre en la legislación estadística.

Manifestó que el Instituto al que representa realizó un diagnóstico de la actual legislación en relación al Sistema Estadístico Nacional. A partir de lo anterior, explicó que se elaboraron las siguientes observaciones:

a) ley N° 19.628, sobre protección de la vida privada y protección de datos de carácter personal.

i.- Señala en su artículo 1º: “El tratamiento de datos de carácter personal en registros o bancos de datos por organismos públicos (…) se sujetará a las disposiciones de esta ley”.

Explicó que el mencionado cuerpo legal no reconoce la especialidad de normas referidas al tratamiento de datos estadísticos. Atendido lo anterior, solicitó que la iniciativa en estudio lo consagre.

ii.- El Título IV: Se refiere al tratamiento de datos por parte de los organismos públicos, regulación que resulta ser insuficiente teniendo en vista las funciones que cumple el INE. Detalló que el mencionado instituto levanta información de encuestas o de registros administrativos. Remarcó que toda vez que la información esté en manos del Estado se debe maximizar el esfuerzo para no solicitarla nuevamente.

Lo anterior, argumentó, no favorece la cesión de datos entre organismos públicos y ello afecta el principio de eficiencia estadística.

iii.- Esta iniciativa no contempla la excepción estadística en materia de tratamiento de datos personales, lo que también afecta el principio de eficiencia estadística.

En relación a los aspectos positivos del proyecto presentado por el Ejecutivo, destacó los siguientes:

i.- Establece en su Art. 1º su carácter supletorio de reglas especiales, lo que parece apropiado, en contraposición a la ley vigente.

ii.- Consagra ampliamente la excepción estadística, específicamente en los siguientes artículos:

- Artículo 5°: Derecho de Acceso (no debe obstaculizar tratamiento con fines estadísticos).

- Art 7°, letra d): Derecho de Cancelación (no procede si el tratamiento es para fines estadísticos).

- Art 8°, letra d): Derechos de Oposición (no procede si el tratamiento es para fines estadísticos)

- Art 16 bis, letra d): Datos personales relativos a salud (tratamiento lícito para fines estadísticos).

iii.- El Art. 20 consagra una regla de incalculable valor para la administración pública.

- Facilita la interoperabilidad de las bases de datos, la coordinación entre los servicios que también tienen atribuciones estadísticas y significa un salto en eficiencia del uso de los datos en poder del Estado, y

- Fortalece los principios de: Coordinación, Eficiencia y Costo-Efectividad, Pertinencia, Calidad técnica. (Principios de ONU, 2014).

Luego, sostuvo que existen países como Suecia y Holanda, que hace veinte años cuentan con la interoperabilidad y el resultado de lo anterior es que, por ejemplo, Suecia no realiza encuestas. Agregó que la mayor parte de su información la obtiene de sus registros administrativos. Aseveró que los países más desarrollados no efectúan censos, sino que solo recopilan información basada en registros administrativos.

En seguida, destacó que el Instituto Nacional de Estadísticas trabaja con los mayores resguardos de confidencialidad. Precisó que el mencionado instituto cuenta con un secreto estadístico cuya vulneración trae aparejada una sanción penal. Remarcó que si el INE recibe una base de datos nominada, una vez que se incorpora en sus estadísticas, se elimina el nombre asociado a ella.

Admitió que le genera ciertas aprehensiones el inciso primero del artículo 16 sexies de la iniciativa del Ejecutivo, porque dependiendo de cómo se interprete, pudiera eliminar lo positivo de las reglas antes mencionadas.

En él se señala: “Datos personales con fines históricos, estadísticos, científicos y de estudios o investigaciones. Las personas naturales o jurídicas, de derecho público o privado, podrán tratar datos personales con fines históricos, estadísticos, científicos y para estudios o investigaciones que atiendan fines de interés público, cuando el titular haya prestado su consentimiento en forma inequívoca, específica, previa e informada.”

Dada la anterior redacción, sugirió borrar la expresión “públicos” por 2 razones:

1.- Los organismos públicos tienen una regulación especial en el proyecto, y

2.- Este artículo establece en su inciso final una exigencia demasiado compleja y contradictoria si los cedentes y cesionarios son organismos públicos.

Reiteró que la redacción comentada viene a limitar todas las ventajas mencionadas anteriormente.

Finalizó su intervención valorando el proyecto del Ejecutivo en lo que dice relación con la actividad estadística.

IDEA DE LEGISLAR

Concluidas las audiencias ya transcritas, **el Presidente de la Comisión, Honorable Senador señor Harboe**, puso en votación la idea de legislar sobre esta iniciativa.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, De Urresti, Harboe y Larraín, aprobó en general este proyecto de ley.

DISCUSIÓN EN PARTICULAR

Seguidamente, **el señor Presidente de la Comisión** sometió a discusión en particular el proyecto de ley, iniciado en Mensaje de S.E. la Presidenta de la República, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales (Boletín 11.144-07) y el proyecto de ley, iniciado en Moción de los Honorables Senadores señores Harboe, Araya, De Urresti, Espina y Larraín, sobre protección de datos (Boletín N° 11.092-07).

Como se ha indicado previamente, la Comisión acordó utilizar como punto de partida para este este trabajo, el proyecto de ley presentado por el Ejecutivo.

Hacemos presente que respecto de cada norma que se analiza siempre se tuvo a la vista las disposiciones contenidas en la mencionada Moción. Asimismo, los integrantes de la Comisión propusieron enmiendas a las normas en debate, tal como sucede durante el análisis en particular de una iniciativa de ley.

Al iniciarse el estudio de esta materia, **el Presidente de la Comisión, Honorable Senador señor Harboe,** ofreció la palabra al **asesor del Ministerio de Hacienda, señor Roberto Godoy**.

El señor Godoy recordó que la Comisión de Constitución, Legislación, Justicia y Reglamento solicitó a un equipo técnico integrado por asesores de los Honorables Senadores de esta Comisión y por representantes del Poder Ejecutivo, que formulare proposiciones que permitieran integrar ambas iniciativas.

Connotó que fruto de dicho trabajo se elaboró un conjunto de propuestas que se someterán a la consideración de la Comisión y que tienen como base el texto del proyecto de ley del Ejecutivo. Asimismo, aclaró que las mismas recogen las ideas contenidas en el Mensaje del Ejecutivo, con excepción de dos aspectos. El primero dice relación con el Título III de la ley N° 19.628, que consiste en la regulación de los datos económicos. El segundo, se refiere a la institucionalidad. Recordó que solo el Mensaje desarrolla esta materia, asunto que no fue objeto de debate pormenorizado por parte de los asesores de los parlamentarios y del Gobierno.

Aclarado lo anterior, la Comisión dio inicio al estudio de ambas iniciativas de ley y de las mencionadas propuestas.

Artículo Primero

Esta disposición del proyecto de ley del Ejecutivo introduce diversas enmiendas a la referida ley Nº 19.628.

Número 1)

Este precepto modifica el artículo 1° de la ley N° 19.628.

La norma vigente dispone que el tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares se sujetará a las disposiciones de esta ley, con excepción del que se efectúe en ejercicio de las libertades de emitir opinión y de informar, el que se regulará por la ley a que se refiere el artículo 19, N° 12, de la Constitución Política.

Agrega que toda persona puede efectuar el tratamiento de datos personales, siempre que lo haga de manera concordante con esta ley y para finalidades permitidas por el ordenamiento jurídico. En todo caso deberá respetar el pleno ejercicio de los derechos

fundamentales de los titulares de los datos y de las facultades que esta ley les reconoce.

Al iniciarse el estudio de esta materia, **Presidente de la Comisión, Honorable Senador Harboe**, puso en discusión el número 1) del artículo primero del proyecto de ley presentado por el Ejecutivo.

Esta disposición sustituye el referido artículo por el siguiente:

“Artículo primero.- Introdúcense las siguientes modificaciones a la ley Nº 19.628, sobre protección de la vida privada:

1) Reemplázase el artículo 1° por el siguiente:

“Artículo 1.- Objeto y ámbito de aplicación. La presente ley tiene por objeto regular el tratamiento de los datos personales que realicen las personas naturales o jurídicas, públicas o privadas, con el propósito de asegurar el respeto y protección de los derechos y libertades de quienes son titulares de estos datos, en particular, el derecho a la vida privada.

Todo tratamiento de datos personales que realicen las personas naturales o jurídicas, incluidos los órganos públicos, que no se encuentre regido por una ley especial quedará sujeto a las disposiciones de esta ley. Con todo, en los asuntos no regulados en las leyes especiales se aplicarán supletoriamente las normas de esta ley.

El régimen de tratamiento y protección de los datos personales establecidos en esta ley no se aplicará al tratamiento de datos que realicen los medios de comunicación social en el ejercicio de las libertades de emitir opinión y de informar regulado por las leyes a que se refiere el artículo 19 N° 12 de la Constitución Política de la República, ni al que efectúen las personas naturales en relación con sus actividades personales.”.

Por su parte, la Moción que hemos indicado precedentemente, propone una nueva disposición para regular este asunto. En ella se establece lo siguiente:

“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.”.

En relación a esta materia, el grupo de asesores parlamentarios y los representantes del Ejecutivo, encabezados por la señora Bernardita Piedrabuena y el señor Roberto Godoy, sugirió a los integrantes de la Comisión aprobar el texto propuesto por el Ejecutivo, enmendado en los siguientes términos.

“Artículo primero. Introdúcense las siguientes modificaciones a la ley Nº 19.628, sobre protección de la vida privada:

1) Reemplázase el artículo 1° por el siguiente:

“Artículo 1°.- Objeto y ámbito de aplicación. La presente ley tiene por objeto regular el tratamiento de los datos personales que realicen las personas naturales o jurídicas, públicas o privadas, con el propósito de asegurar el respeto y protección de los derechos y libertades de las personas naturales que son titulares de estos datos, en particular, el derecho a la vida privada.

Todo tratamiento de datos personales que realice una persona natural o jurídica, incluidos los órganos públicos, cuando no se encuentre regido por una ley especial, quedará sujeto a las disposiciones de esta ley. En los asuntos no regulados en leyes especiales, se aplicarán supletoriamente las normas de esta ley.

El régimen de tratamiento y protección de datos establecidos en esta ley no se aplicará al tratamiento de datos que se realice en el ejercicio de las libertades de emitir opinión y de informar reguladas por las leyes a que se refiere el artículo 19 N° 12 de la Constitución Política de la República. Los medios de comunicación social quedarán sujetos a las disposiciones de esta ley en lo relativo al tratamiento de datos que efectúen con una finalidad distinta a la de opinar e informar.

Tampoco serán aplicables las normas de la presente ley al tratamiento de datos que efectúen las personas naturales en relación con sus actividades personales.”.

Al iniciarse el estudio de esta materia, **el Presidente de la Comisión, Honorable Senador Harboe** propuso a la Comisión considerar, en primer lugar, el texto del inciso primero contenido en el número 1) del artículo primero propuesto por el Ejecutivo.

Sobre esta materia, concedió el uso de la palabra al **asesor del Ministerio de Hacienda, señor Godoy,** quien manifestó que el objeto de la ley es, en primer lugar, dar protección a ciertos derechos de las personas, en particular el que se vincula con el derecho a la vida privada y, en segundo lugar, regular el tratamiento de los datos personales. Añadió que ambos propósitos se refunden en el presente proyecto.

Asimismo, destacó que la redacción alternativa propuesta por el grupo de asesores parlamentarios viene a precisar que el sujeto de protección son las personas naturales.

En seguida, intervino **el Honorable Senador señor Larraín,** quien consideró que en lo esencial dicha redacción no cambia el postulado que contiene la Moción, porque con ella se busca regular el tratamiento de los datos personales que realicen personas naturales o jurídicas, públicas o privadas, pero con el propósito de garantizar la protección de los datos, la vida privada de las personas naturales. Por lo tanto, indicó que la regulación se hace en función de un objetivo. Se mostró de acuerdo con la propuesta y ratificó que en la propuesta del grupo de asesores se mantiene el objeto de la presente iniciativa.

Puesto en votación el inciso primero del artículo 1°, contenido en el número 1) del proyecto del Ejecutivo, fue aprobado, incorporando las sugerencias presentadas por el grupo de asesores, por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Larraín y Moreira.

Inciso segundo.

Como se ha indicado precedentemente, el texto del Mensaje, propone considerar como inciso segundo del artículo 1° de la ley N° 19.628, lo siguiente:

“Todo tratamiento de datos personales que realicen las personas naturales o jurídicas, incluidos los órganos públicos, que no se encuentre regido por una ley especial quedará sujeto a las

disposiciones de esta ley. Con todo, en los asuntos no regulados en las leyes especiales se aplicarán supletoriamente las normas de esta ley.”.

Por su parte, en la Moción se señala en esta materia lo siguiente:

“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.”.

En relación con esta materia, el grupo de asesores parlamentarios sugirió a los Senadores de la Comisión aprobar el texto del Ejecutivo, enmendado en los siguientes términos:

“Todo tratamiento de datos personales que realice una persona natural o jurídica, incluidos los órganos públicos, cuando no se encuentre regido por una ley especial, quedará sujeto a las disposiciones de esta ley. En los asuntos no regulados en leyes especiales, se aplicarán supletoriamente las normas de esta ley.”.

Al iniciarse su análisis, el **asesor del Ministerio de Hacienda, señor Godoy,** expresó que el proyecto de ley presentado por el Ejecutivo constituye un marco general regulatorio para el tratamiento de datos personales, y actúa supletoriamente respecto de aquellas entidades que tengan normas específicas sobre el tratamiento de datos. Aseveró que un ejemplo de esto último corresponde a la regulación del seguro de cesantía.

El Presidente de la Comisión, Honorable Senador señor Harboe, enfatizó que este punto es relevante, por cuanto lo que se busca con este proyecto es que se materialice el objetivo contenido en el inciso primero del artículo en estudio. Es decir, que se realice el tratamiento de datos, pero que se asegure el derecho de las personas a protegerlos.

Añadió que resulta lógico el carácter supletorio de esta ley, porque existen tratadores especiales de datos. Detalló que un ejemplo de lo anterior lo constituye el Ministerio Público y las policías. Sostuvo que si a estos últimos se los sometiera a una legislación general, como la que se pretende crear, se podría producir alguna dificultad, porque hay tratamientos diferenciados. No obstante lo anterior, estimó que es partidario de aprobar el texto sugerido por el grupo de asesores parlamentarios, pero dejando abierta la opción de incorporar más adelante un capítulo especial dedicado al tratamiento de datos comerciales.

El Honorable Senador señor Larraín se mostró de acuerdo con la redacción sugerida. Sin embargo, manifestó su preocupación respecto a la falta de regulación de los datos personales almacenados en bases de datos domésticas.

El asesor del Ministerio de Hacienda, señor Godoy explicó que ello se encuentra regulado en este mismo artículo, pero en el inciso subsiguiente.

Concluido el estudio de esta disposición, **el señor Presidente de la Comisión** dio por cerrado el debate.

Puesto en votación el inciso segundo del artículo 1° propuesto por el Ejecutivo, enmendado en los términos sugerido por el grupo de asesores, fue aprobado por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Larraín y Moreira.

Inciso tercero.

A continuación, **el Presidente de la Comisión** sometió a debate el inciso tercero del artículo 1° propuesto en el proyecto presentado por el Ejecutivo. En dicha disposición se establece lo siguiente:

“El régimen de tratamiento y protección de los datos personales establecidos en esta ley no se aplicará al tratamiento de datos que realicen los medios de comunicación social en el ejercicio de las libertades de emitir opinión y de informar regulado por las leyes a que se refiere el artículo 19 N° 12 de la Constitución Política de la República, ni al que efectúen las personas naturales en relación con sus actividades personales.”

En relación a esta materia, se tuvo presente que la Moción propone la siguiente redacción:

“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”.

Por su parte, el grupo de asesores parlamentarios sugirió a la Comisión aprobar el texto del Ejecutivo, enmendado en los siguientes términos:

“El régimen de tratamiento y protección de datos establecidos en esta ley no se aplicará al tratamiento de datos que se realice en el ejercicio de las libertades de emitir opinión y de informar reguladas por las leyes a que se refiere el artículo 19 N° 12 de la Constitución Política de la República. Los medios de comunicación social quedarán sujetos a las disposiciones de esta ley en lo relativo al tratamiento de datos que efectúen con una finalidad distinta a la de opinar e informar.”.

Al iniciarse el estudio de esta materia, **el asesor del Ministerio de Hacienda, señor Godoy,** consignó que en el Mensaje se excluye el tratamiento de datos personales que realicen los medios de comunicación cuando ejercen la libertad de opinión y de informar. Agregó que en la Moción se amplía la mencionada exclusión, y ello es recogido en el texto que propone el grupo de asesores.

Además, explicó, se precisa, tal como lo hace la Moción, que los medios de comunicación se regirán por la presente ley cuando realicen tratamiento de datos para una finalidad distinta a la de opinar e informar.

Puesto en votación el inciso tercero, del artículo 1° del texto del Ejecutivo, fue aprobado en los términos propuestos por el grupo de asesores, por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Larraín y Moreira.

Seguidamente, **el Presidente de la Comisión, Honorable Senador señor Harboe**, hizo presente que el grupo de asesores parlamentarios sugiere a la Comisión incorporar un inciso cuarto, nuevo, al artículo 1°de la ley N° 19.628. Dicha proposición es la siguiente:

“Tampoco serán aplicables las normas de la presente ley al tratamiento de datos que efectúen las personas naturales en relación con sus actividades personales.”

Puesto en votación este nuevo inciso cuarto del artículo 1°, fue aprobado por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Larraín y Moreira.

A continuación, se analizó la propuesta contenida en la Moción que se refunde en el presente informe que incorpora un nuevo

artículo 2° a la ley Nº 19.628. Este precepto determina el ámbito de aplicación territorial de la ley.

En ella se propone lo siguiente: “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.”.

El Presidente de la Comisión, Honorable Senador señor Harboe precisó que el texto refundido no recoge la extraterritorialidad de la ley en esta materia. Aseveró que con posterioridad se regula en el proyecto de ley del Ejecutivo la transferencia internacional de datos.

En virtud de este antecedente, la Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Harboe, Larraín y Moreira, rechazó este precepto.

Número 2)

A continuación, la Comisión estudió las modificaciones que el proyecto de ley del Ejecutivo sugiere introducir al artículo 2° de la ley N° 19.628.

Esta disposición define una serie de conceptos que utiliza la ley. Entre ellos destacan los siguientes: almacenamiento de datos; bloqueo de datos; comunicación o transmisión de datos, dato caduco, dato estadístico; dato de carácter personal, datos sensibles, eliminación o cancelación de datos; fuentes accesibles al público, modificación de datos, organismos públicos, procedimiento de disociación de datos; registro o banco de datos; responsable del registro o banco de datos, titular de datos, y tratamiento de datos.

El proyecto del Ejecutivo introduce una serie de cambios a este precepto. Al respecto sugiere, en primer lugar, lo siguiente:

“2) Modifícase el artículo 2° del siguiente modo:

a) Intercálase el siguiente epígrafe:

“Definiciones.”.

Esta enmienda fue aprobada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Larraín y Moreira.

Seguidamente, se analizó la propuesta contenida en la letra b) del artículo 2º del proyecto de ley del Ejecutivo. Ella reemplaza las letras c), f), g) e i) del artículo 2° de la ley vigente.

Al iniciarse el estudio de esta materia, **el Presidente de la Comisión, Honorable Senador Harboe,** sometió a debate la nueva letra c) que reemplazaría a la letra c) vigente. El texto propuesto por el Ejecutivo es el siguiente:

“c) Comunicación o transmisión de datos personales: dar a conocer por el responsable de datos, de cualquier forma, datos personales a personas distintas del titular a quien conciernen los datos, sin llegar a cederlos o transferirlos. Las comunicaciones que realice el responsable de datos deben contener información exacta, completa y veraz.”.

Sobre esta misma materia, la Moción propone incorporar un artículo 3° nuevo a la ley N° 19.628, que sustituye completamente el artículo 2° de dicha ley, incorporando una serie de nuevas definiciones relativas a que se entiende, por ejemplo, por datos personales, datos sensibles, tratamiento de datos, elaboración de perfiles, procedimiento de disociación de datos, base de datos, fuentes de acceso público, titular, responsable del tratamiento de datos, encargado del tratamiento de datos, intermediarios en el tratamiento de datos, destinatarios, tercero, consentimiento, violación de la seguridad, datos genéticos, datos biométricos, datos relativos a la salud, organismos públicos, y transferencia internacional de datos.

En relación a este asunto, el grupo de asesores parlamentarios sugirió a la Comisión seguir las normas propuestas en el Ejecutivo en su Mensaje, con algunas enmiendas. En virtud de ello, propuso aprobar el siguiente texto:

“c) Comunicación o transmisión de datos personales: dar a conocer por el responsable de datos, de cualquier forma, datos personales a personas distintas del titular a quien conciernen los datos, sin llegar a cederlos o transferirlos. Las comunicaciones que realice el responsable de datos deben contener información exacta, completa y veraz.”.

El Presidente de la Comisión, Honorable Senador señor Harboe señaló que la Moción viene a reemplazar el artículo 2º de la ley N° 19.628, y no hace referencia, ni reconoce las definiciones del mencionado cuerpo legal, sino que elabora un catálogo nuevo. Agregó que el Mensaje solo modifica aquellas definiciones que en la actual legislación no son adecuadas.

Seguidamente, consultó al Ejecutivo que si un motor de búsqueda, como *Google*, publica una determinada información sobre una persona, se entenderá que la mencionada empresa es responsable de datos o un intermediario.

El asesor del Ministerio de Hacienda, señor Godoy, señaló que la consulta formulada está vinculada con la definición de responsable de datos. Añadió que lo que caracteriza al responsable es que tome decisiones acerca de los medios y fines del tratamiento de datos. Según el caso planteado, si *Google* está tomando decisiones respecto de la información que se está entregando, será calificado como responsable. Si la mencionada empresa solo actúa como intermediario, como canal, no estará tomando decisiones respecto de los medios o fines.

Recalcó que la discusión se debe resolver caso a caso, pero lo relevante es el carácter finalista del examen que se realiza.

Puesta en votación la letra c) del texto del proyecto del Ejecutivo, enmendada en los términos sugeridos por el grupo de asesores parlamentarios, fue aprobada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Larraín y Moreira.

En seguida, la Comisión examinó la nueva **letra f)** contenida en el Mensaje del Ejecutivo. Ella señala lo siguiente:

“f) Dato personal: cualquier información vinculada o referida a una persona natural, identificada o identificable a través de medios que puedan ser razonablemente utilizados.”

Por su parte, el grupo de asesores sugirió reemplazar la letra f) propuesta por el Ejecutivo por la siguiente:

“f) Dato personal: cualquier información vinculada o referida a 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, excluyendo aquellos casos en que el esfuerzo de identificación sea desproporcionado.”.

Al iniciarse el estudio de esta proposición, **el asesor del Ministerio de Hacienda, señor Godoy,** precisó que el grupo de asesores propone un cambio relevante en la definición de dato personal. Remarcó que éste es uno de los aspectos claves de la iniciativa en discusión. Reconoció que en la elaboración del concepto se recogió parte importante de lo que en esta materia propone la Moción que se refunde en este proyecto, precisamente con el objeto de determinar cuándo se considera que una persona es identificable. Agregó que el estándar propuesto en el Mensaje consistía en que éste se realice a través de medios que puedan ser razonablemente utilizados. Lo anterior generaba bastante incertidumbre a la hora de decidir. Afirmó que la definición de dato personal de la Moción es más clara.

Hizo presente que respecto a este tema, la Excma. Corte Suprema, en su oficio de respuesta a la consulta que formuló el Senado, manifestó lo siguiente:

“La definición propuesta parece ambigua por dos razones. Primero, porque no especifica claramente qué es aquello que podría constituir la razonabilidad del medio empleado para relacionar un dato específico de una base de datos con una persona. ¿Se refiere a la razonabilidad del esfuerzo o el trabajo empleado?, ¿se refiere al tiempo de cómputo que implica el medio de identificación? o ¿se refiere a la imposibilidad de realizar la identificación mediante medios automatizados? Segundo, porque al adoptar este nuevo criterio -y asumiendo que es posible aislar un concepto de razonabilidad del medio que resulte jurídicamente operativo-, la definición propuesta amenaza con disminuir los estándares de protección actualmente vigentes, incentivando la generación de espacios (resquicios) en los que podría darse un tratamiento abusivo de datos, en tanto no cabrían en la definición de dato personal propuesta por la ley. Ello, en la medida que el responsable del tratamiento demuestre que el medio que empleó para identificar al titular del dato fue arduo, difícil u oneroso y, por lo tanto, a través de un medio que no responda al concepto de “razonablemente utilizado”.

Dado lo anterior, **el señor Godoy** constató que el concepto elaborado en la Moción otorga mayor certeza jurídica a los

operadores en el área del tratamiento de datos. Al respecto recordó que el texto de la Moción define a los datos personales en los siguientes términos:

"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;"

El Presidente de la Comisión, Honorable Senador señor Harboe, señaló que también otorga certeza a los ciudadanos, saber cuáles son sus datos de carácter personal y conocer el nivel de protección de los mismos. Recordó que el dato personal permite identificar a una persona, directa o indirectamente. Recalcó que la propuesta constituye un avance respecto a lo que existe hoy.

El Honorable Senador señor Larraín consignó que el camino planteado en la Moción es más claro que el contenido en el Mensaje. Declaró que la materia en estudio va evolucionando con el desarrollo de las tecnologías.

Sugirió agregar la expresión "tales como", antes de la frase "el número de cédula de identidad,", con la finalidad de enfatizar que se trata de una enumeración de elementos que podrían caracterizar el identificador.

El Presidente de la Comisión, Honorable Senador señor Harboe coincidió con la idea de añadir la expresión señalada por el Honorable Senador señor Larraín, para que se entienda que es una enumeración meramente ejemplar. Aseveró que la evolución de la ciencia generará nuevos desafíos que deberán ser considerados como dato personal.

A continuación, le ofreció la palabra **al asesor del Honorable Senador señor Larraín, señor Héctor Mery**.

El señor Mery estimó razonable el cambio propuesto. Constató que las palabras utilizadas en la Moción no son las mismas que las del texto sugerido por el grupo de asesores. Preguntó si en él, cuando se habla de elementos de la identidad cultural o social, se entienden comprendidas las convicciones religiosas; filosóficas; afiliación sindical y datos relativos a la salud; vida y orientación sexual.

El Presidente de la Comisión, Honorable Senador señor Harboe aclaró que al incorporar la expresión "tales como",

se amplía el ámbito de protección. Aseveró que los elementos planteados por el señor Mery quedan incorporados.

Puesta en votación la definición de "dato personal" propuesto por Ejecutivo, fue aprobado en los términos sugeridos por el grupo de asesores, con la última enmienda señalada. Se pronunciaron a favor la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Araya, Harboe, Larraín y Moreira.

A continuación, la Comisión trató la propuesta del proyecto de ley del Ejecutivo de sustituir la **letra g)** del artículo 2º de la ley Nº 19.628.

La norma vigente define qué se entiende por datos sensibles.

En relación a este asunto, el proyecto de ley del Ejecutivo sugiere la siguiente redacción:

"g) Datos personales sensibles: aquellos datos personales que conciernen o se refieren a las características físicas o morales de una persona, tales como el origen racial, ideología, afiliación política, creencias o convicciones religiosas o filosóficas, estado de salud físico o psíquico, orientación sexual, identidad de género e identidad genética y biomédica.".

Por su parte, la Moción de los parlamentarios propone definir datos sensibles en los siguientes términos:

"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.".

En relación con este asunto, el grupo de asesores parlamentarios sugirió a la Comisión aprobar el proyecto del Ejecutivo, enmendado en los siguientes términos:

"g) Datos personales sensibles: aquellos datos personales que revelen el origen étnico o racial, las opiniones políticas, la afiliación política, sindical o gremial, las convicciones ideológicas o filosóficas, las creencias religiosas, los datos relativos a la salud, al perfil biológico humano, los datos biométricos, y la información relativa a la vida

sexual, a la orientación sexual y a la identidad de género de una persona natural.”.

Al iniciarse el estudio de esta materia, **el Presidente de la Comisión, Honorable Senador señor Harboe,** hizo presente que la Moción hace referencia a las consecuencias que puede traer a una persona el tratamiento de cierta información y acompaña una extensa enumeración a modo ejemplar. Dado lo anterior, afirmó que se siguió la doctrina europea que es la que se consigna en lo propuesto por el grupo de asesores parlamentarios.

El asesor del Ministerio de Hacienda, señor Godoy, precisó que el grupo de asesores revisó la legislación comparada y, a partir de las audiencias desarrolladas por la Comisión, llegaron a la convicción de que era importante ampliar el catálogo, con la finalidad de otorgar mayor certeza. Enfatizó que no se puede dejar entregado a la subjetividad de una persona el determinar si un dato es sensible.

El Honorable Senador señor Larraín advirtió que no es fácil resolver las diferencias que se suscitan en esta materia. Mostró su inquietud respecto a la fórmula propuesta por el texto elaborado por el grupo de asesores parlamentarios, porque busca, a través, de un catálogo cerrado definir cuándo estamos en presencia de datos sensibles. Añadió que su inclusión no necesariamente los constituye en datos sensibles.

Se preguntó por qué se considera dato sensible la opinión política de una persona. Aseveró que la Moción identificaba un criterio que tiene dos elementos, el primero, cuando el tratamiento implique discriminación arbitraria o ilegal, y el segundo, cuando conlleve un grave riesgo para la intimidad de su titular.

Asimismo, **el Honorable Senador, señor Moreira** consultó por la naturaleza de la cédula nacional de identidad.

El asesor del Ministerio de Hacienda, señor Godoy respondió que esta última es considerada como dato personal.

El Honorable Senador, señor Moreira constató que éste puede ser utilizado por cualquier persona para obtener cualquier tipo de información fraudulenta.

El Presidente de la Comisión, Honorable Senador señor Harboe, manifestó que la intimidad constituye el origen del derecho a la protección de datos. Por tanto, lo que persigue el concepto de dato sensible es un mayor nivel de resguardo legal. Agregó que existen ciertas esferas de la intimidad, que la persona legítimamente tiene el derecho a que no sean conocidas. Añadió que si las personas son individuos que se

dedican a asuntos públicos, y pertenecen a una asociación política; sindical; religiosa, y lo manifiestan expresamente, significa que voluntariamente están ejerciendo el derecho de revelar su pertenencia a este tipo de asociaciones.

Afirmó que también hay un conjunto de ciudadanos que no siendo personeros públicos, no desean que se sepa que pertenecen, por ejemplo, a determinada iglesia o a un partido político. Recalcó que es legítimo respetar esa esfera de intimidad.

Subrayó que si la persona considera que los datos mencionados forman parte de la esfera de su intimidad, se deben proteger con especial énfasis, porque las consecuencias de su eventual vulneración pueden ser complejas.

Estimó positivo que se incorporen elementos que no estaban considerados en la Moción, como son el perfil biológico y los datos biométricos. Recordó que la legislación vigente, dentro del catálogo que establece para definir dato sensible, habla de estados de salud físico o psíquico. Expresó que la evolución de la ciencia ha llevado a que hoy en el hemisferio norte sea común la realización de estudios genéticos, y estos pueden revelar ciertas predisposiciones a cierto tipo de enfermedades.

Sostuvo que se puede dar el caso de una empresa que se dedique a hacer exámenes genéticos y que es adquirida por una compañía de seguro. La información será transmitida a esta última y ello llevará a que la empresa de seguros tome decisiones relacionadas con los estudios genéticos, llegando, por ejemplo, a negar la contratación de un seguro a una determinada persona.

Respecto a si la norma en discusión es abierta o cerrada, mostró su preocupación con que sea abierta, porque puede generar la tentación de que en la práctica se vaya eliminando el carácter de dato personal y que éste sea considerado como dato sensible.

La Coordinadora de Finanzas Internacionales y Mercado de Capitales del Ministerio de Hacienda, señora Bernardita Piedrabuena, justificó que la norma propuesta por el grupo de asesores parlamentarios sugiera una lista cerrada, porque al definir dato sensible los estándares para su tratamiento se elevan. Detalló que tratándose de estos datos el consentimiento que debe ser expreso y las multas que se le aplican a un responsable de datos, son más elevadas. Por lo tanto, afirmó, que el responsable de datos debe tener claridad respecto a la naturaleza del dato que está manejando.

En relación a la cédula nacional de identidad, remarcó que se decidió que éste no tuviera la calidad de dato sensible, sino que actúa como identificador.

El asesor del Honorable Senador señor Larraín, señor Olmedo, expresó que una de las medidas a considerar en el resto del articulado consiste en determinar cómo esta legislación recoge efectivamente el derecho fundamental de la protección de datos.

Constató que hay una definición que está ausente en materia de datos sensibles, a saber, los hábitos personales. Estos últimos los encontramos como excepción al principio de transparencia, en la Ley sobre Acceso a la Información Pública. Apuntó que dichos hábitos constituyen una de las grandes matrices por las cuales se puede proceder a la transferencia de datos posteriormente. Se mostró partidario que éstos se incorporen en la definición.

Asimismo, señaló que la afiliación gremial no responde a la categoría de dato sensible, a diferencia de la sindical.

El Presidente de la Comisión, Honorable Senador señor Harboe propuso aprobar la letra g), con algunas enmiendas.

Consideró que las opiniones políticas no debieran ser catalogadas como datos sensibles, sí la afiliación política. Estimó que hay dos elementos que no están incorporados a la definición propuesta por el grupo de asesores y que están contemplados en la legislación vigente, a saber, las características físicas y los hábitos personales. Se mostró partidario que se incluyan estos elementos en la definición de datos sensibles.

El Honorable Senador señor Larraín se mostró partidario de que si la lista que se elabora es cerrada, se debe dejar abierta una posibilidad adicional, como por ejemplo, utilizando la siguiente fórmula: “y también cuando esa información esté destinada a producir una discriminación arbitraria o ilegal”

La Coordinadora de Finanzas Internacionales y Mercado de Capitales del Ministerio de Hacienda, señora Bernardita Piedrabuena, recordó que en la exposición que hizo el Ministerio de Hacienda al inicio de la discusión de la presente iniciativa, se recalcó que se deben proteger los datos personales, pero al mismo tiempo se debe permitir el traspaso de información que es indispensable para el flujo económico, más aún en la era de la globalización y de los medios digitales.

Mostró su preocupación respecto a la idea de incorporar, bajo el concepto de datos sensibles, los hábitos personales, porque es un concepto muy amplio y se termina restringiendo la libre circulación de la información.

El Honorable Senador, señor Moreira precisó que no es conveniente dejar abierto dicho término, ya que puede dar lugar a interpretaciones contradictorias, situación que consideró riesgosa. Estimó que las opiniones políticas no están en la esfera de la intimidad.

El Presidente de la Comisión, Honorable Senador señor Harboe, constató que los parlamentarios tienen una conocida adscripción política, pero no sucede lo mismo con un individuo que trabaja en otro lugar y pertenece a un partido político y quiere que su afiliación no se divulgue. Lo mismo puede suceder con su orientación sexual.

Agregó que la ley no consagra una prohibición, sino que determina qué datos tendrán la categoría de sensible. Ello significa que el nivel de protección será mayor.

Hizo presente que una de las diferencias entre el dato personal y el dato personal sensible, consiste en que mientras el primero admite consentimiento expreso y tácito; el sensible solo admite el consentimiento expreso para su tratamiento.

Sostuvo que si se deja la puerta medianamente abierta, puede llevar a frenar la posibilidad del flujo de datos que son importantes en la economía colaborativa. Remarcó que el objetivo que se persigue no es solo proteger los datos de las personas, sino que también consiste en no frenar dicha economía, evitando el traspaso de la información.

El Honorable Senador señor Larraín manifestó que si se sigue el criterio de la lista cerrada, es razonable excluir las opiniones políticas de los datos sensibles. Aseveró que si existe una opinión es porque alguien la ha emitido, la ha exteriorizado voluntariamente. Reconoció que situación distinta ocurre con la afiliación a un partido político.

En cuanto a los hábitos personales, afirmó que dicho concepto está regulado por la actual legislación. Preguntó si ello ha sido factor de complicación, si ha obstruido el flujo de datos que debe existir.

En este mismo ámbito, **el Honorable Senador, señor Moreira** preguntó de qué manera se puede frenar una publicación en Wikipedia.

El Presidente de la Comisión, Honorable Senador señor Harboe, recordó que Wikipedia seguirá informando. Advirtió que el problema radica en que si en dicho sitio web aparece un dato sensible, el afectado tendrá derecho a solicitar que sea eliminado.

El asesor del Ministerio de Hacienda, señor Godoy, connotó que de la definición actual de dato sensible, lo que ha

generado mayor controversia, desde el punto de vista de su aplicación, son las expresiones de características morales y hábitos personales, porque éstos se remiten a conductas subjetivas difíciles de precisar.

Añadió que los datos sensibles tienen una protección reforzada, en términos que solo pueden ser utilizados por un tercero con el consentimiento expreso del titular de esos datos. Por lo tanto, argumentó, el sujeto que trata datos requiere tener certeza acerca de qué información tiene esta condición especial. Desde esa perspectiva, en el texto propuesto por el grupo de asesores, se excluye características morales y hábitos personales.

La Coordinadora de Finanzas Internacionales y Mercado de Capitales del Ministerio de Hacienda, señora Bernardita Piedrabuena manifestó que no se debe olvidar que la legislación vigente en muchos casos no se cumple. Apreció que incorporar la expresión “hábitos personales” puede llevar a dificultar el flujo de información en la economía.

El asesor del Honorable Senador señor Larraín, señor Olmedo, afirmó que extraer hábitos personales de datos sensibles, significa pensar una modificación a la Ley sobre Acceso a la Información Pública.

El asesor del Comité Udi, señor Héctor Mery manifestó cierta incertidumbre respecto a considerar “hábito personal” como dato personal sensible, en la medida que hay mercados que requieren información.

Agregó que un estudio de mercado necesita conocer hábitos de consumo y el público se beneficia del mismo.

Se mostró partidario de la postura expresada en el texto propuesto a la Comisión por el grupo de asesores.

El Presidente de la Comisión, Honorable Senador señor Harboe sugirió votar el texto propuesto por el grupo de asesores, eliminando la expresión “las opiniones políticas”, e incorporando “las características físicas”.

La Coordinadora de Finanzas Internacionales y Mercado de Capitales del Ministerio de Hacienda, señora Bernardita Piedrabuena constató que la información sobre las características físicas constituye un dato útil para el flujo de la economía, ya que muchas veces se hacen ofertas productos tomando en consideración dichos aspectos.

El asesor del Ministerio de Hacienda, señor Godoy señaló que el hecho de que las características físicas y los hábitos

personales no sean considerados como dato personal sensible, no significa que no sean datos personales y que no estén protegidos por la legislación.

En virtud de la precisión anterior, **el Presidente de la Comisión, Honorable Senador señor Harboe**, sometió a votación la letra g) propuesta por el grupo de asesores, suprimiendo la expresión “las opiniones políticas”.

Puesta en votación la letra g), en los términos ya indicados, fue aprobada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Araya, Harboe, Larraín y Moreira.

El Honorable Senador señor Larraín sugirió se incorporen los hábitos personales como dato personal sensible. Fundamentó su propuesta, indicando que se debe proteger la intimidad de las personas, y la incorporación de este concepto facilita la protección de sus datos.

A continuación se sometió a votación la propuesta del Honorable Senador señor Larraín, de incluir como dato personal sensible, la expresión “hábitos personales”.

Sometida a votación, se pronunció a favor el Honorable Senador, señor Larraín. En contra lo hizo el Honorable Senador, señor Harboe. Se abstuvieron, los Honorables Senadores, señores Araya y Moreira.

El Presidente de la Comisión, Honorable Senador señor Harboe fundamentó su voto, expresando que los hábitos personales constituyen un dato personal y estarán protegidos.

Dado este resultado, y en aplicación de lo prescrito en el artículo 178 del Reglamento del Senado, se repitió la votación. A favor de su aprobación lo hizo el Honorable Senador señor Larraín. Se pronunciaron en contra, los Honorables Senadores, señores Araya y Harboe. Se abstuvo el Honorable Senador señor Moreira.

Repetida la votación se mantuvo en los términos ya descritos, razón por la que se dio por rechazada esta proposición.

Seguidamente, **el señor Presidente de la Comisión** puso en discusión la enmienda **a la letra i) del artículo 2º de la ley Nº 19.628**, que define fuentes de acceso público.

En esta materia, el proyecto de ley del Ejecutivo propone lo siguiente:

“i) Fuentes de acceso público: todas aquellas bases de datos personales, públicas o privadas, cuyo acceso o consulta puede ser efectuado en forma lícita por cualquier persona, sin existir restricciones o impedimentos legales para su acceso o utilización.

Las dudas o controversias que se susciten sobre si una determinada base de datos es considerada fuente de acceso público serán resueltas por la Agencia de Protección de Datos Personales, quien podrá identificar categorías genéricas, clases o tipos de registros o bases de datos que posean esta condición.”.

En relación con esta misma materia, la Moción presentada por los Senadores propone lo siguiente:

“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.”.

En relación a esta materia, el grupo de asesores parlamentarios sugirió a la Comisión aprobar el texto del Ejecutivo, enmendado en los siguientes términos:

“i) Fuentes de acceso público: todas aquellas bases de datos o conjuntos de datos personales, públicos o privados, cuyo acceso o consulta puede ser efectuada en forma lícita por cualquier persona, siempre que no existan restricciones o impedimentos legales para su acceso o utilización.”.

Al iniciarse el estudio de esta materia, **el Presidente de la Comisión, Honorable Senador señor Harboe,** ofreció la palabra **al asesor del Ministerio de Hacienda, señor Godoy,** quien manifestó que la propuesta del Ejecutivo define fuente de acceso público, mientras que en la Moción se busca crear un catálogo cerrado de lo que entendería por ello.

Precisó que estamos ante un tema que puede variar en el tiempo y no es conveniente establecer un catálogo estricto. Se mostró partidario de definir claramente cuándo estamos en presencia de fuente de acceso público.

Agregó que los cambios tecnológicos y las propias normas van generando nuevos registros de carácter público que son imposibles de consignar en una lista cerrada.

Sostuvo que la propuesta que elaboró el Ministerio de Hacienda y que fue recogida por el grupo de asesores parlamentarios, consiste en establecer los estándares técnicos para definir una fuente de acceso público. Agregó que cuando un titular o responsable de datos tenga duda respecto de si una determinada fuente, es o no de acceso público, deberá recurrir a la Agencia de Protección de Datos para que determine, en base a los parámetros que le entrega la ley, si ella reúne los requisitos para ser considerada como tal.

El Presidente de la Comisión, Honorable Senador señor Harboe, consultó cuál será el grado de responsabilidad de aquellos que mantienen datos en este tipo de fuentes.

Consignó que, por ejemplo, en la Moción se enumeraba, como fuente de acceso público, al Censo Nacional de Población y Vivienda del Instituto Nacional de Estadísticas. Constató que la ley que regula a este Instituto establece responsabilidad por los datos que administra.

Asimismo, hizo presente que puede existir una fuente de acceso público que se haya construido sobre la base de alguno de los principios, como el de licitud y que, con posterioridad, dichos datos pueden ser utilizados con un fin distinto por el cual se recolectaron.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena recordó que el artículo 13, letra a) del texto que se analizará más adelante, prescribe lo siguiente:

“Artículo 13.- Otras fuentes de licitud del tratamiento de datos. Es lícito el tratamiento de datos personales, sin el consentimiento del titular, en los siguientes casos:

a) Cuando los datos han sido recolectados de una fuente de acceso público y su tratamiento esté relacionado con los fines para los cuales fueron entregados o recogidos.”.

Estimó que con esta disposición se otorga una mayor protección al titular de los datos. Precisó que también se consagra el derecho de oposición cuando se utilicen los datos del titular con un fin distinto al autorizado.

El asesor del Honorable Senador señor Larraín, señor Olmedo, consultó si la declaración por parte de la Agencia de si una información proviene de una fuente de acceso público, tiene efectos *erga omnes*. Dado lo anterior, preguntó si estamos en presencia de una acción popular.

En segundo término, sugirió fortalecer dicha declaración, dado el impacto que tendrá. Afirmó que ella debiese ser considerada dentro de las obligaciones de transparencia activa de la nueva Agencia y ser publicada, a lo menos, en su página *web*.

El Presidente de la Comisión, Honorable Senador señor Harboe hizo presente que el inciso segundo de la letra i) del texto del proyecto propuesto por el Mensaje dispone lo siguiente:

“Las dudas o controversias que se susciten sobre si una determinada base de datos es considerada fuente de acceso público serán resueltas por la Agencia de Protección de Datos Personales, quien podrá identificar categorías genéricas, clases o tipos de registros o bases de datos que posean esta condición.”.

Consultó si esa norma se repite en el texto refundido.

El asesor del Ministerio de Hacienda, señor Godoy, explicó que no se considera en el texto sugerido por el grupo de asesores parlamentarios pues en la letra o) del nuevo artículo 31, que define las funciones y atribuciones de la Agencia de Protección de Datos Personales, se especifica que corresponder a este organismo:

“o) Resolver las dudas o controversias que se susciten sobre si una determinada base de datos es considerada fuente de acceso público e identificar categorías genéricas, clases o tipos de datos, conjuntos de datos o bases de datos que posean esta condición.”.

Reconoció que en el grupo de asesores se produjo una larga discusión respecto de consagrar acciones populares o fundamentadas en interés difuso, en materia de protección de datos. Recordó que la esencia del bien jurídico protegido es la privacidad de las personas. Por lo tanto, arguyó, éste se funda en el interés personal de quien se pueda sentir afectado por la información, tomada de determinada fuente, es o no de acceso público. Ratificó que el grupo de asesores no visualizó que exista sustento jurídico que nos permita diseñar o introducir una acción amplia o de carácter popular. Advirtió que distinto es lo que ocurre en el caso de los consumidores donde se puede entender que respecto de una publicidad o de un determinado producto, se puedan ver afectadas distintas personas.

Adicionalmente, manifestó que se estableció expresamente, como causales del derecho de oposición, cuando el tratamiento tenga origen en fuente de acceso público. Añadió que si un titular de datos siente que ese tratamiento obedece a una fuente que no tiene dichas características puede ejercer este derecho y hacer que cese el tratamiento de sus datos.

El Presidente de la Comisión, Honorable Senador señor Harboe, sostuvo que, como se examinará más adelante, el artículo 38 del proyecto del Ejecutivo considera dicha hipótesis como una infracción grave a esta ley. Su texto es el siguiente:

“a) Tratar los datos personales sin contar con el consentimiento del titular de datos o sin una base que otorgue licitud al tratamiento, o tratarlos con una finalidad distinta de aquella para la cual fueron recolectados.”

Consignó que, de esta manera, se establece la facultad de la Agencia de Protección de Datos y el carácter de grave de la infracción.

Aclarado lo anterior, el señor Presidente de la Comisión puso en votación **la letra i) del artículo 2º propuesta por Ejecutivo, enmendada en los términos sugeridos por el grupo asesores, la cual fue aprobada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Araya, Harboe y Larraín.**

Con la misma votación se aprobó la propuesta del Ejecutivo de eliminar la letra j) del artículo 2° de la ley N° 19.628, pasando la actual letra k) a ser j), y así sucesivamente.

En seguida, la Comisión consideró las sustitución de las letras l), m), n), ñ) y o) que pasan a ser letra k), l), m) y n) y ñ)

A continuación, **el Presidente de la Comisión, Honorable Senador señor Harboe**, puso en discusión **la nueva letra k) del artículo 2º** de la ley Nº 19.628, contenida en el Mensaje del Ejecutivo.

Su texto es el siguiente:

"k) Proceso de anonimización o disociación: procedimiento en virtud del cual los datos personales no pueden asociarse al titular ni permitir su identificación, por haberse destruido el nexo con toda información que lo identifica o porque dicha asociación exige un esfuerzo no razonable, entendiendo por tal el empleo de una cantidad de tiempo, gasto o trabajo desproporcionados. Un dato anonimizado deja de ser un dato personal.".

En relación con esta materia, la Moción presentada por los Senadores propone en su artículo 3º la siguiente disposición:

"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;".

En relación con esta materia, el grupo de asesores de los parlamentarios sugirió a la Comisión aprobar el texto del Ejecutivo, enmendado en los siguientes términos:

"k) Proceso de anonimización o disociación: procedimiento en virtud del cual un dato personal no pueden vincularse o asociarse a una persona determinada, ni permitir su identificación, por haberse destruido o eliminado el nexo con la información que vincula, asocia o identifica a esa persona. Un dato anonimizado deja de ser un dato personal.".

Al iniciarse el estudio de esta letra, **el asesor del Ministerio de Hacienda, señor Godoy,** aseveró que no hay una diferencia sustantiva entre lo que dispone el Mensaje y el texto propuesto por el grupo de asesores de los parlamentarios. Afirmó que en este último consagra una regla más clara, respecto a la propuesta inicial del Ejecutivo, en términos de establecer que el proceso de anonimización consiste en aquel en que se rompe el vínculo que permite identificar la información con una persona determinada, identificada o identificable.

Agregó que en esta definición se reitera una regla que señala que un dato anonimizado deja de ser un dato personal.

Hizo presente que hoy es prácticamente imposible establecer un proceso completo de anonimización o disociación.

Concluida esta explicación, **el señor Presidente de la Comisión** puso en votación la letra k) del texto del Ejecutivo, enmendada en los términos propuesto por el grupo de asesores parlamentarios.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó esta propuesta.

A continuación, **el Presidente de la Comisión** puso en discusión **la nueva letra l) del artículo 2º de la ley Nº 19.628** contenida en el proyecto de ley del Ejecutivo. Su texto es el siguiente:

“l) Base de datos personales: conjunto organizado de datos personales, cualquiera sea la forma o modalidad de su creación, almacenamiento, organización y acceso, que permita relacionar los datos entre sí, así como realizar el tratamiento de ellos.”.

En relación con este asunto, la Comisión tuvo en cuenta que la Moción, en su artículo 3°, número 6, señala lo siguiente:

“6) Base de datos: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados.”.

Sobre este aspecto, el grupo de asesores parlamentarios sugirió a la Comisión aprobar el siguiente texto:

“l) Base de datos personales: conjunto organizado de datos personales, cualquiera sea la forma o modalidad de su creación, almacenamiento, organización y acceso, que permita relacionar los datos entre sí, así como realizar el tratamiento de ellos.”

Al comenzar el estudio de esta disposición, **el asesor del Ministerio de Hacienda, señor Godoy,** expresó que estamos ante una definición estándar. Precisó que esta regla amplía el concepto de base de datos estructurada.

El Honorable Senador señor Larraín compartió esta propuesta y sugirió redactar la última frase del párrafo de la siguiente manera: “así como realizar su tratamiento.”.

Puesta en votación la nueva letra l) del artículo 2º propuesto por Ejecutivo, en los términos sugeridos por el grupo de asesores parlamentarios y con la enmienda propuesta por el Honorable Senador Larraín, fue aprobada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Araya, Harboe y Larraín.

Seguidamente, **el Presidente de la Comisión, Honorable Senador señor Harboe,** puso en discusión **la nueva letra m) del artículo 2º,** contenido en el proyecto del Ejecutivo. Su texto es el siguiente:

“m) Responsable de datos o responsable: persona natural o jurídica, pública o privada, a quien compete decidir acerca del tratamiento de datos personales, con independencia de si los datos son tratados directamente por él o a través de un tercero o mandatario, y de su localización.”

En relación con esta materia, la Moción de los Senadores propone, en su artículo 3º, lo siguiente:

“9) Responsable del tratamiento o responsable: la persona natural o jurídica que, solo o junto con otros, determine los fines y medios del tratamiento;”

Por su parte, el grupo de asesores parlamentarios propuso aprobar el texto del Ejecutivo enmendado en los siguientes términos:

“m) Responsable de datos o responsable: toda persona natural o jurídica, pública o privada, que decide acerca de los fines y medios del tratamiento de datos personales, con independencia de si los datos son tratados directamente por ella o a través de un tercero mandatario o encargado.”.

Al comenzar el estudio de estas propuestas, **el asesor del Ministerio de Hacienda, señor Godoy,** señaló que la redacción elaborada por el grupo de asesores recoge algunas de las ideas establecidas en la Moción, fundamentalmente en lo que dice relación con la idea de establecer un estándar para efectos de determinar quién es el responsable de datos. Afirmó que el mencionado estándar consiste en que es responsable de datos, aquel que toma la decisión acerca de los fines y medios del tratamiento, y no necesariamente quien efectúa el tratamiento.

El Presidente de la Comisión, Honorable Senador señor Harboe, estimó que ésta era una definición muy importante. Aseveró que existe una discusión respecto a si las empresas que ponen los datos a disposición de los usuarios, son responsables de los mismos.

Destacó que se amplía el ámbito de responsabilidad, lo que le parece adecuado para evitar que se produzca una cadena de responsabilidades y que obliguen al titular del dato a perseguir a un responsable que no conoce.

Agregó que esta definición también dice relación con la categoría de infracciones, porque cuando se revisa su catálogo, específicamente el artículo 38 del proyecto de ley del Ejecutivo, nos encontramos con la siguiente disposición: “Las infracciones a los principios y obligaciones establecidos en esta ley cometidas por los responsables de datos se califican, atendida su gravedad, en leves, graves y gravísimas.”.

Lo anterior tiene incidencia en la determinación de la responsabilidad y las sanciones que se pueden aplicar.

El Honorable Senador señor Larraín consultó por qué en el texto propuesto por el Ejecutivo se utiliza el término “localización”.

El asesor del Ministerio de Hacienda, señor Godoy, recalcó que la localización nos introduce en dos dimensiones, una que dice relación con el lugar donde se ubica el responsable, y otra que consiste en el lugar donde están alojados los datos que serán objeto del tratamiento.

Agregó que independiente de la localización del responsable, o donde estén alojados los datos, es responsable aquel que efectúa un tratamiento, definiendo los fines y medios del mismo.

Consignó que el tratamiento de datos que se realiza en Chile, independiente de su localización, se encuentran sujetos al ordenamiento jurídico nacional, por aplicación del principio de territorialidad de la ley.

El asesor del Comité Udi, señor Héctor Mery destacó que el término localización genera duda en cuanto a que pudiera entenderse que la legislación chilena pretende regular a sujetos que se encuentran fuera del territorio nacional.

El asesor del Ministerio de Hacienda, señor Godoy, hizo presente que en el ámbito del tratamiento de datos es donde se producen mayores dificultades a la hora de determinar la jurisdicción, porque muchos tratamientos de datos de personas que residen en el territorio nacional, se realiza por responsables que están instalados en otras jurisdicciones.

Afirmó que en esta materia se han seguido dos orientaciones normativas. Una corresponde a Europa, que consiste en que

independiente del domicilio del responsable de datos, si se tratan datos de ciudadanos amparados bajo la legislación europea, se aplica esta última.

Precisó que en Latinoamérica se ha optado por seguir la normativa de aplicación estricta de la territorialidad de la ley.

Subrayó que en el texto propuesto por el grupo de asesores se busca mantener una regla de aplicación de la legislación chilena a aquellos tratamientos de datos que se realicen en Chile por nacionales o extranjeros.

Añadió que el término localización no es indispensable incorporarlo, ya que bastaría con aplicar las reglas generales de la legislación nacional, específicamente la consagrada en el artículo 14 de nuestro Código Civil.

El Presidente de la Comisión, Honorable Senador señor Harboe, apuntó que la utilización del término localización es importante para efectos de la transferencia internacional de datos.

Manifestó que el artículo 28 del proyecto de ley de Ejecutivo señala que:

“La Agencia de Protección de Datos Personales podrá autorizar la transferencia internacional de datos, siempre que el transmisor y el receptor de los datos otorguen las garantías adecuadas en relación con la protección de los derechos de las personas que son titulares de estos datos y la seguridad de la información transferida. La Agencia de Protección de Datos Personales podrá imponer condiciones previas para que se verifique la transferencia.

Corresponderá al responsable de datos que efectuó la transferencia internacional de datos, acreditar que ésta se practicó de conformidad a las reglas establecidas en esta ley.”.

Sostuvo que dado lo prescrito, es importante incorporar el concepto de localización.

El Honorable Senador señor Larraín sostuvo que mantiene su inquietud, porque, en definitiva, se está hablando de quién es el responsable de la base de datos. Consultó si este último también lo es de la localización de la mencionada base. Constató que no siempre es así. Estimó que no es necesario utilizar este término en esta disposición.

Aseveró que lo importante es la responsabilidad de toda persona natural o jurídica que decide acerca de los fines y modos de tratamiento de los datos personales, más que su localización.

El asesor del Ministerio de Hacienda, señor Godoy, connotó que lo central en este debate es quién decide acerca de los fines y medios del tratamiento, con independencia de quien efectúa el tratamiento materialmente.

El Honorable Senador señor Larraín determinó que debe quedar claro cuál es el sentido de incorporar el término "localización.".

El asesor del Comité Udi, señor Héctor Mery consignó que el término localización confunde, por lo tanto, lo recomendable sería eliminarlo.

El asesor del Ministerio de Hacienda, señor Godoy, insistió que lo importante es que exista nitidez respecto de quien es el responsable. Éste es quien define los medios y fines del tratamiento, independiente de quién lo ejecuta o del lugar donde se encuentra el que ejecuta su tratamiento.

De acuerdo a lo señalado**, el Presidente de la Comisión, Honorable Senador señor Harboe,** puso en votación **la letra m) del artículo 2º contenida en el proyecto del Ejecutivo,** en los términos sugeridos por el grupo de asesores parlamentarios, con la supresión de la expresión**:** ", y de su localización.".

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, De Urresti, Harboe y Larraín, aprobó esta propuesta.

Seguidamente, la Comisión estudió la propuesta del proyecto de ley del Ejecutivo que propone incorporar **la siguiente letra n)** al artículo 2° de la ley N°19.628

"n) Titular de datos o titular: persona natural, identificada o identificable, a quien conciernen o se refieren los datos personales."

Por su parte la Moción de los Senadores, define esta materia, en su artículo 3º, en los siguientes términos:

"8) Titular: la persona a la que se refieren los datos de carácter personal.".

Luego de un breve intercambio de opiniones, en que se consideró más clara la propuesta del Gobierno, **el Presidente de la**

Comisión, Honorable Senador señor Harboe, puso en votación el texto del Ejecutivo.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores, señores Araya, De Urresti, Harboe y Larraín, aprobó esta redacción.

Seguidamente, **el señor Presidente de la Comisión** sometió a debate **la letra ñ)** contenida en el Mensaje del Ejecutivo. Su texto es el siguiente:

"ñ) Tratamiento de datos: cualquier operación o conjunto de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, procesar, almacenar, comunicar, transmitir o utilizar de cualquier forma los datos personales.".

En relación a esta materia, la Moción de los Senadores señala lo siguiente:

"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;"

Por su parte, el grupo de asesores parlamentarios sugirió a la Comisión aprobar el texto del Ejecutivo, con una enmienda final:

"ñ) Tratamiento de datos: cualquier operación o conjunto de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, procesar, almacenar, comunicar, transmitir o utilizar de cualquier forma datos personales o <u>conjuntos de datos personales</u>.".

Al iniciarse el estudio de esta disposición, **el asesor del Ministerio de Hacienda, señor Godoy,** advirtió que esta definición era muy importante para este proyecto de ley.

Por su parte, **el Presidente de la Comisión, Honorable Senador señor Harboe,** se mostró de acuerdo con la redacción sugerida por el grupo de asesores parlamentarios.

En virtud de lo anterior, puso en votación el texto del Ejecutivo, con la enmienda sugerida por el grupo de asesores de los parlamentarios.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, De Urresti, Harboe y Larraín, aprobó esta disposición.

En seguida, **el señor Presidente de la Comisión** sometió a consideración la nueva letra o) que se incorpora al artículo 2º de la ley 19.628. En ella se define que se entiende por consentimiento. Su texto es el siguiente:

"o) Consentimiento: toda manifestación de voluntad libre, específica, inequívoca e informada mediante la cual el titular de datos, su representante legal o mandatario, según corresponda, autoriza el tratamiento de los datos personales que le conciernen.

Por su parte, la Moción de los Senadores define esta materia en el artículo 3º, en los siguientes términos:

"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;".

El Presidente de la Comisión, Honorable Senador Harboe, puso en votación el texto propuesto por el proyecto de ley del Ejecutivo.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, De Urresti, Harboe y Larraín, aprobó esta proposición. Asimismo, dio por subsumida en esta redacción las ideas contenidas en el texto de la Moción.

A continuación, **el señor Presidente de la Comisión**, puso en discusión la nueva letra p) contenida en el proyecto de ley del Ejecutivo. En ella se regula el derecho al acceso.

Su texto establece lo siguiente:

"p) Derecho de acceso: derecho del titular de datos a solicitar y obtener del responsable confirmación acerca de si sus datos personales están siendo tratados por él, acceder a ellos en su caso, y a la información prevista en esta ley."

Puesta en votación la letra p) del texto del proyecto de ley del Ejecutivo, fue aprobada por la unanimidad de los

miembros presentes de la Comisión, Honorables Senadores señores Araya, De Urresti, Harboe y Larraín.

A continuación, **el señor Presidente de la Comisión** puso en discusión **la letra q)** del artículo 2° contenido en el Mensaje del Ejecutivo. Su texto es el siguiente:

"q) Derecho de rectificación: derecho del titular de datos a solicitar y obtener del responsable que modifique o complete sus datos personales, cuando están siendo tratados por él y sean inexactos o incompletos."

El grupo de asesores parlamentarios expresó que respaldaba el texto propuesto por el Ejecutivo.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, De Urresti, Harboe y Larraín, aprobó esta disposición.

Seguidamente, la Comisión examinó **la letra r)** contenida en las enmiendas que el proyecto de ley del Ejecutivo formula al artículo 2° de la ley N° 19.628. Su texto es el siguiente:

"r) Derecho de cancelación: derecho del titular de datos a solicitar y obtener del responsable que suprima o elimine sus datos personales, de acuerdo a las causales previstas en la ley."

Al iniciarse el estudio de esta modificación, **el asesor del Comité Udi, señor Héctor Mery,** consultó si el derecho de cancelación corresponde a lo que se denomina derecho al olvido.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena manifestó que no son sinónimos. Constató que el derecho al olvido se hace efectivo mediante la cancelación.

Concluido el análisis de esta modificación, **el señor Presidente de la Comisión** la sometió a votación.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, De Urresti, Harboe y Larraín, aprobó esta letra del proyecto de ley del Ejecutivo.

Luego, **el Presidente de la Comisión, Honorable Senador señor Harboe**, sometió a consideración de la Comisión la propuesta del Ejecutivo para consignar la siguiente letra s) en el artículo 2° de la ley N° 19.628. En ella se regula el denominado derecho de oposición.

“s) Derecho de oposición: derecho del titular de datos que se ejerce ante el responsable con el objeto de requerir que no se lleve a cabo un tratamiento de datos determinado, de conformidad a las causales previstas en la ley.”.

Al iniciarse el estudio de esta materia, **el asesor del Ministerio de Hacienda, señor Godoy**, hizo presente que el grupo de asesores parlamentarios había acordado sugerir que se apruebe esta norma, enmendada en el siguiente sentido:

“s) Derecho de oposición: derecho del titular de datos a solicitar y obtener del responsable, que no se lleve a cabo un tratamiento de datos determinado, de conformidad a las causales previstas en la ley.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores, señores Araya, De Urresti, Harboe y Larraín, aprobó el texto del Ejecutivo, enmendado en los términos indicados precedentemente.

A continuación, **el señor Presidente de la Comisión, Honorable Senador señor Harboe**, sometió a consideración de la Comisión la incorporación de una nueva letra t), contenida en el proyecto de ley del Ejecutivo, que regula el derecho a la portabilidad de los datos personales. Su texto es el siguiente:

“t) Derecho a la portabilidad de los datos personales: derecho del titular de datos a solicitar y obtener del responsable en un formato electrónico estructurado, genérico y de uso habitual, una copia de sus datos personales y comunicarlos o transferirlos a otro responsable de datos”.

En relación a esta materia, el grupo de asesores parlamentarios sugirió a los Senadores aprobar esta norma en los siguientes términos:

“t) Derecho a la portabilidad de los datos personales: derecho del titular de datos a solicitar y obtener del responsable, una copia de sus datos personales en un formato electrónico estructurado, genérico y común, que permita ser operado por distintos sistemas, y poder comunicarlos o transferirlos a otro responsable de datos.”

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, De Urresti, Harboe y Larraín, aprobó el texto del Ejecutivo, enmendado en los términos indicados precedentemente.

Seguidamente, **el señor Presidente de la Comisión** puso en discusión la proposición del Ejecutivo para incorporar una letra u), nueva al mencionado artículo 2°, que crea el Registro Nacional de Cumplimiento y Sanciones. Su texto es el siguiente:

"u) Registro Nacional de Cumplimiento y Sanciones: registro nacional de carácter público administrado por la Agencia de Protección de Datos Personales, que consigna las sanciones impuestas a los responsables de datos por infracción a la ley, los modelos de prevención de infracciones que implementen los responsables y los programas de cumplimiento debidamente certificados.".

Al iniciarse el debate de esta norma, **el Honorable Senador señor Larraín** solicitó una explicación mayor sobre el mencionado Registro, y especialmente su relación con el artículo 4° transitorio del texto del Ejecutivo, que prescribe que: "Dentro de los sesenta días anteriores a la entrada en vigencia de las modificaciones a la ley N° 19.628, sobre protección de la vida privada, contenida en el artículo primero de la presente ley, el Servicio de Registro Civil e Identificación deberá eliminar el registro de bases de datos personales contemplado en el actual artículo 22 de la ley N° 19.628.".

El asesor del Ministerio de Hacienda, señor Godoy, explicó que el registro que se propone crear tiene por objeto mantener información sobre los responsables de datos que hayan sido sancionados por la autoridad de control, en virtud de una infracción a la ley N° 19.628 sobre protección de datos de carácter personal. Además, contiene el listado de aquellos responsables de datos que desarrollen y presenten un modelo de cumplimiento. Agregó que esta propuesta recoge las recomendaciones de la OCDE en esta materia, e incentiva fuertemente el principio de responsabilidad. Por lo tanto, continuó, consagra la posibilidad de que los responsables de datos puedan desarrollar procedimientos de auto cumplimiento y de auto regulación, que son certificados y acreditados por la autoridad de control.

En relación a la norma transitoria ya mencionada, connotó que en el contexto de la iniciativa en estudio, existía la posibilidad de constituir un registro de responsables de datos, y de bases de datos, que es lo que actualmente existe en el Registro Civil, respecto a los organismos públicos.

Expresó que la ley N° 19.628 dispuso que dichos organismos, que tengan bases de datos reguladas por ley de tratamiento de datos, deben registrar tales bases en el Servicio de Registro Civil e Identificación.

Reconoció que la tendencia mundial es ir abandonando los sistemas de registro, porque prácticamente todas las actividades económicas efectúan actividades de tratamiento de datos. Por lo tanto, argumentó, tendríamos que enrolar a todas las entidades públicas.

El Presidente de la Comisión, Honorable Senador señor Harboe, se mostró partidario de contar con un sistema de registro. Para justificar lo anterior, relató lo sucedido con la ley que regula el *lobby* y las gestiones que representen intereses particulares ante las autoridades y funcionarios. Constató que actualmente no existe un registro de lobistas y la carga recae sobre las autoridades públicas y no sobre el sujeto activo. Reconoció que existe un conjunto de instituciones que ejercen labores de representación de intereses, pero no se reconocen como tales.

Agregó que debe haber una oferta unívoca del Estado en esta materia. Puntualizó que es necesario crear una instancia a la que pueda recurrir el ciudadano para verificar si está en una base de datos. Destacó que esta idea corresponde a una manifestación del derecho de acceso.

Asimismo, consideró relevante que el mencionado registro contemple los modelos de prevención de infracciones que deben implementar los responsables de datos. Igualmente, alabó que se consignen en este registro las sanciones, ya que ello actuará como un incentivo para que se mejoren los estándares de calidad del tratamiento de datos. Además, el mencionado registro debería dar cuenta si el modelo de prevención implementado por un tratador de datos se encuentra certificado.

El Honorable Senador señor Larraín manifestó que aprobar el registro en estudio no es incompatible con mantener el que existe en el Servicio de Registro Civil.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena, expresó que los titulares de datos no se encuentran desamparados, porque existe una obligación de transparencia de información de los responsables de datos. Propuso que ella sea activa. Además, precisó que la mencionada obligación no reemplaza el registro, pero permitirá saber si una empresa es tratadora de datos.

El asesor del Comité Udi, señor Héctor Mery, indicó que es interesante la referencia que se ha hecho en este debate a la aplicación de la ley que regula el *lobby*. Reconoció que cuando se aprobó dicha normativa, si bien no se creó un sistema como el que aquí se propone, sí se establecieron los registros de audiencia. A partir de ellos, se elabora y se extrae información relevante, sin tener que acudir a otra instancia.

Se mostró contrario a incrementar el número de registros, ya que su utilidad no está demostrada. Respecto a los modelos de prevención, se preguntó si es necesario que consten en un registro.

El Presidente de la Comisión, Honorable Senador señor Harboe, consignó que en relación al *lobby* existe un conjunto de instituciones que se autodenominan de asesoría legislativa y que tienen financiamiento de empresas. Constató que es indispensable tomar conocimiento de esa situación. Recalcó que en la medida que el *lobby* cuente con un registro, éste adquirirá mayor transparencia.

Respecto a la presente iniciativa, connotó que la mejor manera de elevar los estándares se logra incentivando la creación de un registro, donde se incorporen todos los tratadores de datos, para que no se afecten los derechos de los titulares.

Concluido el debate de esta disposición, **el señor Presidente de la Comisión** puso en votación la letra u) del proyecto del Ejecutivo, enmendado de conformidad a la sugerencia formulada por los asesores parlamentarios.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, De Urresti, Harboe y Larraín, aprobó la norma propuesta por el Ejecutivo, en los términos indicados precedentemente.

Artículo 3°

A continuación, la Comisión analizó las normas del proyecto del Ejecutivo que incorporan un conjunto de principios a la ley N° 19.628.

Entre tales principios destacan los siguientes: de licitud del tratamiento de datos, de finalidad, de proporcionalidad, de calidad, de responsabilidad, de seguridad, y de información.

Al iniciarse el estudio de esta materia, **el Presidente de la Comisión, Honorable Senador señor Harboe**, propuso tratar, en primer lugar, el principio de licitud de tratamiento de los datos.

El texto del proyecto de ley del Gobierno propone lo siguiente:

“Artículo 3.- Principios. El tratamiento de los datos personales se rige por los siguientes principios:

a) Principio de licitud del tratamiento. Los datos personales sólo pueden tratarse con el consentimiento de su titular o por disposición de la ley.”

Por su parte, sobre esta materia, la Moción dispone, en su artículo 4°, lo que a continuación se transcribe:

“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 solo 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.”.

En el análisis de este asunto, la Comisión tuvo presente una proposición del grupo de asesores parlamentarios que sugirió aprobar la letra a) del artículo 3° del texto del Ejecutivo, en los siguientes términos:

“a) Principio de licitud del tratamiento. Los datos personales sólo pueden tratarse con sujeción a la ley.”.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, De Urresti, Harboe y Larraín, aprobó el texto del proyecto del Ejecutivo, con la enmienda planteada precedentemente.

A continuación, **el señor Presidente de la Comisión,** puso en debate la letra b), del artículo 3° del proyecto de ley del Ejecutivo. Esta norma dispone lo siguiente:

“b) Principio de finalidad. Los datos personales deben ser recolectados con fines específicos, explícitos y lícitos. El tratamiento de los datos personales debe limitarse al cumplimiento de estos fines.

En aplicación de este principio, no se pueden tratar los datos personales con fines distintos a los informados al momento de la recolección, salvo que el titular otorgue nuevamente su consentimiento, los datos provengan de fuentes de acceso público o así lo disponga la ley.”

En relación con este texto, el grupo de asesores de parlamentarios sugirió a la Comisión aprobar el proyecto de ley del Gobierno enmendado en los siguientes términos:

“b) Principio de finalidad. Los datos personales deben ser recolectados con fines específicos, explícitos y lícitos. El tratamiento de los datos personales debe limitarse al cumplimiento de estos fines.

En aplicación de este principio, no se pueden tratar los datos personales con fines distintos a los informados al momento de la recolección, salvo que el tratamiento sea compatible y para fines relacionados con los autorizados originalmente; exista un contexto y una relación entre el titular y el responsable que justifique el tratamiento de los datos con una finalidad distinta; el titular otorgue nuevamente su consentimiento; los datos provengan de fuentes de acceso público, y cuando lo disponga la ley.”.

Puesto en votación el párrafo primero de la letra b), del artículo 3° del texto sugerido por el grupo de asesores parlamentarios, fue aprobado por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores, señores Araya, De Urresti, Harboe y Larraín.

En el análisis del párrafo segundo, **el Honorable Senador señor Larraín**, preguntó si las distintas hipótesis descritas por esta disposición eran alternativas, o copulativas.

El asesor del Ministerio de Hacienda, señor Godoy, explicó que eran alternativas. Se trata, señaló, de distintas opciones que dan legitimidad al tratamiento de datos, más allá de la finalidad específica por el cual fueron originalmente recolectados.

El Presidente de la Comisión, Honorable Senador señor Harboe, mostró su preocupación sobre esta materia. Indicó que al ser alternativos se genera una gran amplitud, especialmente en el empleo de la expresión: “exista un contexto y una relación entre el titular y el responsable que justifique el tratamiento de los datos con una finalidad distinta”.

La asesora del Ministerio de Economía, señora Piedrabuena, señaló que hay una relación entre el titular y el responsable que recogió determinados datos para ciertos fines. Posteriormente, los mismos responsables, estiman que hay un fin que es compatible con el destino original de esos datos. Agregó que, en lugar de solicitar nuevamente el consentimiento, se lleva a cabo el tratamiento.

Sobre este asunto, **el Presidente de la Comisión, Honorable Senador señor Harboe** ejemplificó con el caso de la farmacia que solicita el número de cédula nacional de identidad para efectuar un descuento y luego esa información es traspasada a una compañía de seguros. Precisó que en esa situación es evidente que hay una entrega de datos con una finalidad distinta a la que se otorgó. Cuando el individuo del ejemplo concurre a la compañía de seguro, la póliza que deberá pagar será más elevada, porque la empresa tendrá conocimiento de las enfermedades que sufre o le pueden afectar.

Sugirió a los representantes del Ejecutivo elaborar una nueva redacción para esta disposición, que permita evitar situaciones como la descrita. Reiteró que las hipótesis que contempla el párrafo segundo de la letra b) son demasiado amplias y deben circunscribirse.

El Honorable Senador, señor Larraín reconoció que de todas las hipótesis que contiene esta disposición, la planteada es la más compleja de entender. Propuso se busque una mejor redacción para esta disposición.

En una sesión posterior, los representantes del Ejecutivo propusieron la siguiente redacción para el párrafo segundo de la letra b):

“En aplicación de este principio, no se pueden tratar los datos personales con fines distintos a los informados al momento de la recolección, salvo que el tratamiento sea para fines compatibles con los

autorizados originalmente; exista una relación contractual o pre contractual entre el titular y el responsable que justifique el tratamiento de los datos con una finalidad distinta; el titular otorgue nuevamente su consentimiento; los datos provengan de fuentes de acceso público, y cuando lo disponga la ley.”.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó la enmienda propuesta por el Ejecutivo.

A continuación, **el señor Presidente de la Comisión** puso en discusión **la letra c) del artículo 3°** del proyecto de ley del Ejecutivo. Esta disposición establece lo siguiente:

“c) Principio de proporcionalidad. Los datos personales que se traten deben limitarse a aquellos que resulten necesarios en relación con los fines del tratamiento.

Los datos personales deben ser conservados sólo por el período de tiempo que sea necesario para cumplir con los fines del tratamiento, luego de lo cual deben ser cancelados o anonimizados. Un período de tiempo mayor requiere autorización legal o consentimiento del titular.”

Sobre esta materia, la Moción parlamentaria propone, en su artículo 8°, letra d), lo siguiente:

“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.”

En relación con este asunto, el grupo de asesores parlamentario sugirió aprobar, sin enmiendas, el texto del proyecto de ley del Gobierno.

Sobre esta proposición, **el asesor del Honorable Senador señor Larraín, señor Olmedo**, manifestó que se debe ratificar el carácter fundamental del derecho a la protección de datos, tal como se consagra el acceso a la información en la ley N° 20.285. Estimó conveniente incorporarlo dentro del principio en estudio.

El Presidente de la Comisión, Honorable Senador señor Harboe, expresó estar de acuerdo en el fondo de lo planteado, pero no se mostró partidario de incorporarlo en el principio de proporcionalidad, porque se restringiría su sentido.

Sugirió que el Ejecutivo considere una propuesta para que en el encabezado de los principios se haga una mención a que el derecho a la protección de datos es un derecho fundamental.

Sometida a votación la letra c) del artículo 3° del proyecto de ley del Ejecutivo, fue aprobada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Araya, Harboe y Larraín.

Seguidamente, **el señor Presidente de la Comisión** puso en discusión la letra d) del artículo 3º, del proyecto de ley del Ejecutivo que establece el principio de calidad. Su texto es el siguiente:

“d) Principio de calidad. Los datos personales deben ser exactos y, si fuera necesario, completos y actuales, en relación con los fines del tratamiento.”.

En relación a esta materia, la Moción parlamentaria que se refunde en este proyecto prescribe, en su artículo 8°, letra c), lo siguiente:

“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.”

Al iniciarse el debate de este asunto, el grupo de asesores parlamentarios sugirió a la Comisión aprobar el proyecto de ley del Gobierno, sin enmiendas.

El Presidente de la Comisión, Honorable Senador señor Harboe, consideró que debe eliminarse la frase: “y si fuera necesario”. Ratificó que los mencionados datos deben ser completos. Asimismo, indicó que la ley vigente utiliza el término veraz.

El asesor del Ministerio de Hacienda, señor Godoy precisó que el estándar que se utiliza es alto. Destacó que la frase observada por el Honorable Senador Harboe se justifica porque existirán situaciones en que el responsable de datos no tendrá toda la información respecto del titular. Afirmó que se exige que los datos sean completos cuando es consustancial a la finalidad del tratamiento. Lo mismo sucede respecto a la actualización de la información.

El Presidente de la Comisión, Honorable Senador señor Harboe, hizo presente que los datos deben ser actuales, porque, a través de ellos, se hacen evaluaciones, y éstos al no estar vigentes, no reflejan el verdadero estado del sujeto. Sostuvo que en la propia definición de dato personal se señala que son aquellos que sirven para identificar una persona dentro de un contexto. Recalcó que la exactitud también dice relación con la actualidad del dato, salvo que se refiera a una actividad de almacenamiento de antecedentes antiguos.

El Honorable Senador señor Larraín aseveró que la redacción complejiza la comprensión del principio en estudio. Agregó que la expresión: "y si fuera necesario", es poco clara. Propuso que se reemplace o se elimine.

El Presidente de la Comisión, Honorable Senador señor Harboe, hizo referencia a lo señalado en la Moción respecto al principio de calidad. Constató que ella exige un mayor y mejor examen.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena, hizo presente que se pueden almacenar datos que estén desactualizados y no ser caducos.

El Presidente de la Comisión, Honorable Senador señor Harboe, consignó que hoy en día existe un conjunto de bases de datos que solo cuentan con el correo electrónico de los titulares. Enfatizó que esa información se considera completa, ya que permite identificar a una persona. Lo anterior no significa que debe tener toda la información. Señaló que un dato no actualizado puede generar una afectación de derechos.

Propuso aprobar la definición elaborada en la Moción, eliminando su parte final. Es decir, el texto que se sugiere es el siguiente:

"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."

El asesor del Ministerio de Hacienda, señor Godoy manifestó que se está definiendo el principio de calidad, que se aplicará para todas las operaciones y actividades de tratamiento de datos. Constató que en la letra c), del artículo 14 del texto que se analizará más adelante, se establece como una de las obligaciones del responsable de datos, lo siguiente:

"c) Comunicar o ceder, en conformidad a las disposiciones de esta ley, información exacta, completa y veraz.".

Agregó que cuando un responsable realiza tratamiento de datos, no necesariamente cuenta con información completa y actualizada. En todo caso, precisó, está obligado a que esa información sea exacta, completa y veraz, cuando la comunica a terceros.

Por otra parte, recordó que existen niveles de información que solo pueden ser obtenidos por la entrega que realice el titular. Consignó que los datos que trate el responsable tienen que ser exactos, lo que constituye un parámetro más objetivo.

El Presidente de la Comisión, Honorable Senador señor Harboe se mostró en desacuerdo con limitar la exactitud de la información. Asimismo, indicó que no solo la comunicación de datos debe ser completa y veraz. Advirtió que esta última es una de las actuaciones a las que ha de tener derecho el tratador de datos, si corresponde.

Enfatizó que la información debe ser de calidad, para cumplir con el objetivo de mejorar los estándares de la industria.

Asimismo, afirmó que la mala calidad de la información pueden llegar a afectar derechos fundamentales. Lo anterior lo ejemplificó con el caso de una persona que ha sido condenada por un delito, que han transcurrido los años necesarios para que ejerza el derecho que establece la ley para poder borrar su condena, y el tenedor de una base de datos no la ha actualizado.

Recalcó que es vital que los antecedentes contenidos en ella, sean veraces y que la mencionada base se encuentre actualizada.

En este punto del debate, **la asesora del Ministerio de Economía, señora Bernardita Piedrabuena,** sugirió la siguiente redacción:

“d) Principio de calidad. Los datos personales deben ser exactos, completos y actuales, en relación con los fines del tratamiento.”.

Puesta en votación la letra d) del artículo 3° del proyecto del Ejecutivo, con la enmienda antes transcrita, fue aprobada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Araya, Harboe y Larraín.

En seguida, se consideró el principio de responsabilidad, establecido en la letra e) del artículo 3º del Ejecutivo. Su texto es el siguiente:

“e) Principio de responsabilidad. Quienes realicen tratamiento de los datos personales serán legalmente responsables del cumplimiento de los principios, obligaciones y deberes de conformidad a esta ley.”.

En relación a esta materia, la Moción parlamentaria que se refunde en este proyecto propone, en su artículo 8º, lo siguiente:

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

Al iniciarse el estudio de este asunto, el grupo de asesores parlamentario propuso recoger este principio en los términos sugeridos por el proyecto de ley del Ejecutivo.

El Presidente de la Comisión, Honorable Senador señor Harboe, preguntó por la redacción de la parte final de la norma del Gobierno, ya que al señalar “de conformidad a esta ley” se podría dar a entender que no es necesario cumplir con las obligaciones que en esta materia establecen otras leyes.

Ante esta inquietud, **la asesora del Ministerio de Economía, señora Piedrabuena,** explicó que el responsable de datos deba dar fiel cumplimiento al resto del ordenamiento jurídico.

Por lo mismo, sugirió a la Comisión modificar la redacción de la parte final del artículo propuesto por el Ejecutivo, reemplazando la expresión “esta”, por “la”.

Puesta en votación la letra e), con la enmienda señalada, fue aprobada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Araya, Harboe y Larraín.

A continuación, **el señor Presidente de la Comisión**, puso en debate el principio de seguridad, establecido en la letra f) artículo 3º del proyecto del Ejecutivo. Su texto es el siguiente:

“f) Principio de seguridad. En el tratamiento de los datos personales se deben garantizar niveles adecuados de seguridad, protegiéndolos contra el tratamiento no autorizado, pérdida, filtración, destrucción o daño accidental y aplicando medidas técnicas u organizativas apropiadas.

En relación a este asunto, la Moción parlamentaria que se refunde en este proyecto propone, en la letra j) de su artículo 8°, lo siguiente:

"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 perdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.".

Al iniciarse el estudio de esta materia, el grupo de asesores parlamentarios, sugirió a la Comisión aprobar el texto del Ejecutivo, enmendado en los siguientes términos:

"f) Principio de seguridad. En el tratamiento de los datos personales, el responsable debe garantizar niveles adecuados de seguridad, protegiéndolos contra el tratamiento no autorizado, pérdida, filtración, daño o destrucción y, aplicando para ello, las medidas técnicas u organizativas apropiadas.

El Presidente de la Comisión, Honorable Senador señor Harboe, recordó que lo que ha hecho la industria es endosar la responsabilidad en el titular de los datos. Ejemplificó con el caso en que se entregan los datos a una empresa que administra una tarjeta de crédito, que cuenta con una clave, y luego, ésta es hackeada. Añadió que frente a esta situación la administradora ofrece un seguro. De esta manera, se subsidia la mala calidad de la seguridad de la empresa.

El asesor del Ministerio de Hacienda, señor Godoy, sostuvo que el principio en estudio se ve reforzado por dos artículos que se analizarán más adelante y que establecen claramente la regulación de las medidas de seguridad, a saber, los artículos 14 quater y 14 quinquies del proyecto de ley del Ejecutivo.

Estas disposiciones prescriben lo siguiente:

"Artículo 14 quater.- Deber de adoptar medidas de seguridad. El responsable de datos debe adoptar las medidas necesarias para resguardar el cumplimiento del principio de seguridad establecido en esta ley, considerando el estado actual de la técnica y los costos de aplicación, junto con la naturaleza, alcance, contexto y fines del tratamiento, así como la probabilidad de los riesgos y la gravedad de sus efectos en relación con el tipo de datos tratados. Las medidas aplicadas por el responsable deben asegurar la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas de tratamiento de datos.

Si las bases de datos que opera el responsable tienen distintos niveles de criticidad, deberá adoptar las medidas de seguridad que correspondan al nivel más alto.

Ante la ocurrencia de un incidente de seguridad, y en caso de controversia judicial o administrativa, corresponderá al responsable acreditar la existencia y el funcionamiento de las medidas de seguridad adoptadas en base a los niveles de criticidad y a la tecnología disponible.”.

“Artículo 14 quinquies.- Deber de reportar las vulneraciones a las medidas de seguridad. El responsable de datos deberá reportar a la Agencia de Protección de Datos Personales, por los medios más expeditos posibles y sin dilaciones indebidas, las vulneraciones a las medidas de seguridad que ocasionen la destrucción, filtración, pérdida o alteración accidental o ilícita de los datos personales que trate o la comunicación o acceso no autorizados a dichos datos, cuando exista un riesgo razonable que con ocasión de estos incidentes se genere un perjuicio o afectación para los titulares.

El responsable de datos deberá registrar estas comunicaciones, describiendo la naturaleza de las vulneraciones sufridas, sus efectos, las categorías de datos y el número aproximado de titulares afectados y las medidas adoptadas para gestionarlas y precaver incidentes futuros.

Cuando dichas vulneraciones se refieran a datos personales sensibles o datos relativos a obligaciones de carácter económico, financiero, bancario o comercial, el responsable deberá también efectuar esta comunicación a los titulares de estos datos. Esta comunicación deberá realizarse en un lenguaje claro y sencillo, individualizando los datos afectados, las posibles consecuencias de las vulneraciones de seguridad y las medidas de solución o resguardo adoptadas. La notificación se deberá realizar a cada titular afectado y si ello no fuere posible, se realizará mediante la difusión o publicación de un aviso en un medio de comunicación social masivo y de alcance nacional.”

El asesor del Comité Udi, señor Héctor Mery connotó que el empleo del término garantizar impone un deber de conducta inexcusable. Por lo tanto, sugirió se utilice la siguiente expresión: “adoptar las medidas razonables de seguridad”.

El Honorable Senador señor Larraín consideró que garantizar corresponde a la obligación y deber que tiene una institución respecto de los compromisos que ha asumido. Agregó que la seguridad de los datos es algo que se busca. Consignó que lo fundamental es lo que se garantiza.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena, recalcó que estamos en presencia de principios. Detalló que en artículos posteriores hay un tratamiento pormenorizado de los mismos.

El asesor del Ministerio de Hacienda, señor Godoy, consideró más apropiado que hablar de “niveles” era mejor utilizar la expresión “estándares adecuados de seguridad”.

Puesta en votación la letra f) del artículo 3° del proyecto del Ejecutivo, según la redacción sugerida por el grupo de asesores parlamentarios, más la última enmienda planteada por el señor Godoy, fue aprobada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Araya, Harboe y Larraín.

Seguidamente, la Comisión consideró el principio de información, contenido en la **letra g) del artículo 3º** del proyecto de ley del Ejecutivo. Su texto es el siguiente:

“g) Principio de información. Las prácticas y políticas sobre el tratamiento de los datos personales deben estar permanentemente accesibles y a disposición de cualquier interesado de manera precisa, clara, inequívoca y gratuita.”.

Al iniciarse el estudio de esta disposición, el grupo de asesores parlamentarios sugirió a la Comisión aprobar este precepto enmendado en los siguientes términos:

“g) Principio de información. Las políticas sobre el tratamiento de los datos personales deben estar permanentemente accesibles y a disposición de cualquier interesado de manera precisa, clara, inequívoca y gratuita.”.

Respecto de esta última proposición, **el asesor del Ministerio de Hacienda, señor Godoy**, expresó que el principio en estudio se encuentra regulado en el artículo 14 ter de esta iniciativa, disposición que trata con detalle el deber de información y transparencia.

Su texto prescribe lo siguiente:

“Artículo 14 ter.- Deber de información y transparencia. El responsable de datos debe mantener permanentemente a disposición del público, en su sitio web o en cualquier otro medio de información equivalente, al menos, la siguiente información:

a) La política de tratamiento de datos personales que ha adoptado, la fecha y versión de la misma.

b) La individualización del responsable de datos, su representante legal, y la identificación del encargado de prevención si existiere.

c) La dirección de correo electrónico, el formulario de contacto o la identificación del medio tecnológico equivalente a través del cual se le notifican las solicitudes que realicen los titulares.

d) Las categorías, clases o tipos de bases de datos que administra; la descripción genérica del universo de personas que comprenden las bases de datos; los destinatarios a los que se prevé comunicar o ceder los datos; y las finalidades del tratamiento que realiza.

e) La política y las medidas de seguridad adoptadas para proteger las bases de datos personales que administra.”

El asesor del Honorable Senador, señor Larraín, señor Olmedo, remarcó que también hay otros artículos donde se impone la obligación de transparencia.

Sugirió emplear la expresión “y las prácticas”, a continuación de “políticas”.

El asesor del Ministerio de Hacienda, señor Godoy consignó que el término propuesto no ha sido utilizado en la presente iniciativa.

Al respecto, **el señor Olmedo** indicó que ello no constituía una buena razón para no emplearlo.

El Presidente de la Comisión, Honorable Senador señor Harboe, preguntó si se usa la expresión “práctica” cuando se configuran los incentivos para lograr autorregulación.

El asesor del Ministerio de Hacienda, señor Godoy, aseveró que no se utiliza. Afirmó que en su lugar se emplea la palabra “medidas”.

El Honorable Senador señor Larraín precisó que, a su juicio, la expresión “medidas” dice relación con las acciones que ejecuta una autoridad y las prácticas constituyen comportamientos desarrollados por distintos grupos.

El Presidente de la Comisión, Honorable Senador señor Harboe, señaló que las políticas se vincula con la idea de las definiciones; las prácticas son los procesos y las medidas corresponden a las acciones. Estimó conveniente incorporar la expresión “prácticas”.

El Honorable Senador señor De Urresti recomendó que el mencionado concepto se aplique en todo el texto legal y no solo en el principio en discusión.

Concluido el debate de este asunto, **el señor Presidente de la Comisión**, puso en votación el siguiente texto:

“g) Principio de información. Las políticas **y las prácticas** sobre el tratamiento de los datos personales deben estar permanentemente accesibles y a disposición de cualquier interesado de manera precisa, clara, inequívoca y gratuita.”.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores De Urresti, Harboe y Larraín, aprobó esta redacción.

A continuación, **el Presidente de la Comisión, Honorable Senador señor Harboe**, consultó a los representantes del Ejecutivo por qué no se consideraron los otros principios que formaban parte del artículo 8º de la Moción Parlamentaria.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena, indicó que, por ejemplo, los principios de minimización de datos y temporalidad se encuentran incorporados en el de proporcionalidad. Agregó que así están tratados, por ejemplo, en la legislación europea. En cuanto al principio de transparencia, precisó que éste se encuentra regulado en la obligación de información y transparencia.

El Presidente de la Comisión, Honorable Senador señor Harboe, señaló que coincidía con los argumentos expresados respecto de los principios de minimización de datos y temporalidad. Sin embargo, explicó que el principio de información, recientemente aprobado, obliga a que los datos sean accesibles a cualquier interesado. Recordó que en esta materia, la Moción, regula el principio de transparencia en la letra e) del artículo 8º. Su texto es el siguiente:

“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.”.

Recalcó que una cosa es que el principio de información obligue al responsable de la base de datos a publicar las políticas y prácticas, y otra cosa distinta es el derecho que tiene el titular de los datos de acceder a la información.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena, aclaró que lo anterior se encuentra recogido en el derecho de acceso. Sin perjuicio de lo anterior, señaló que se podían considerar otros principios contenidos en el texto de la moción.

El Presidente de la Comisión, Honorable Senador señor Harboe, propuso recoger además del principio de transparencia, el de confidencialidad. Su texto es el siguiente:

“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.

El asesor del Honorable Senador señor Larraín, señor Olmedo concordó con lo sugerido. Opinó que en el principio de información ya aprobado, se pueden agregar los principios de transparencia y de confidencialidad.

El Honorable Senador señor Larraín estimó conveniente tratar en primer lugar el principio de información y luego el de transparencia.

Concluido el debate de este asunto, **el Presidente de la Comisión, Honorable Senador señor Harboe**, propuso a la Comisión modificar el texto aprobado precedentemente, para consignar las siguientes letras g) y h), nuevas:

“g) Principio de transparencia e información. Las políticas y las prácticas sobre el tratamiento de los datos personales deben estar permanentemente accesibles y a disposición de cualquier interesado de manera precisa, clara, inequívoca y gratuita.

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.

h) 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.”.

Al iniciarse el debate de estas disposiciones, se propuso aprobarlas en los siguientes términos:

g) Principio de transparencia e información. Las políticas y las prácticas sobre el tratamiento de los datos personales deben estar permanentemente accesibles y a disposición de cualquier interesado de manera precisa, clara, inequívoca y gratuita.

Esta redacción fue aprobada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores De Urresti, Harboe y Larraín.

Seguidamente, se sometió a votación el siguiente párrafo segundo de la letra g)

“El responsable debe adoptar las medidas adecuadas y oportunas para facilitar al titular el acceso a toda la información que señala esta ley, así como cualquier otra comunicación relativa al tratamiento que realiza.”.

Esta redacción fue aprobada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Araya, Harboe y Larraín.

A continuación, **el señor Presidente de la Comisión** puso en discusión la letra h), contenida en el proyecto de ley del Ejecutivo, disposición que establece lo siguiente:

“h) Principio de confidencialidad. El responsable de datos personales y quienes tengan acceso a ellos deberán guardar secreto o confidencialidad acerca de los mismos. El responsable establecerá controles y medidas adecuadas para preservar el secreto o confidencialidad. Este deber subsiste aún después de concluida la relación con el titular.”.

Al iniciarse el debate de este precepto, **los representantes del Ejecutivo, señora Piedrabuena y señor Godoy**, propusieron a la Comisión aprobar el texto del Ejecutivo, enmendado en los siguientes términos:

“h) Principio de confidencialidad. El responsable debe establecer controles y medidas adecuadas para mantener el secreto o confidencialidad acerca de los datos personales que conciernan a un titular. El deber de confidencialidad subsiste aún después de concluida la relación con el titular.”

En relación a esta proposición, **el Honorable Senador señor Larraín** consultó por qué solo subsiste el deber de confidencialidad una vez terminado el vínculo con el titular.

Sugirió la siguiente redacción: “Este deber subsiste aún después de concluida la relación con el titular.”

El Presidente de la Comisión, Honorable Senador señor Harboe se mostró de acuerdo con lo observado por el Honorable Senador señor Larraín.

Preguntó si la obligación del responsable de datos solo consiste en establecer controles y medidas para mantener el secreto o confidencialidad.

Precisó que en el texto de la moción que se refunde en este proyecto, se establecía lo siguiente en relación al deber de 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.”.

Se mostró partidario de consagrar expresamente la obligación de secreto, presente en la redacción precedente, para evitar que se interprete que el responsable cumple con su obligación al establecer controles y medidas.

Constató que el deber de reserva no está recogido en la redacción propuesta por el Ejecutivo.

El asesor del Ministerio de Hacienda, señor Godoy sostuvo que el desarrollo del deber de secreto o confidencialidad está desarrollado extensamente en el artículo 14 bis.

El Presidente de la Comisión, Honorable Senador señor Harboe insistió que en la redacción sugerida a la letra h), no se menciona expresamente la obligación de guardar secreto de los datos.

El Honorable Senador, señor Larraín sugirió a la Comisión aprobar el siguiente texto:

“h) Principio de confidencialidad. El responsable de datos personales y quienes tengan acceso a ellos deberán guardar secreto o confidencialidad acerca de los mismos. El responsable establecerá controles y medidas adecuadas para preservar el secreto o confidencialidad. Este deber subsiste aún después de concluida la relación con el titular.”.

El Presidente de la Comisión, Honorable Senador señor Harboe, concordó con esta proposición y declaró cerrado el debate.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó esta letra, en los términos propuestos por el Honorable Senador Larraín.

Artículo 4º

A continuación, la Comisión consideró el artículo 4º del proyecto de ley del Ejecutivo, que regula los derechos de los titulares de datos personales.

La iniciativa del Gobierno propone modificar el artículo 4º de la ley Nº 19.628, sobre Protección de la Vida Privada.

La norma vigente prescribe que el tratamiento de los datos personales sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello.

Añade que la persona que autoriza debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público.

La autorización debe constar por escrito y puede ser revocada, aunque sin efecto retroactivo, lo que también deberá hacerse por escrito.

Precisa que no requiere autorización el tratamiento de datos personales que provengan o que se recolecten de fuentes accesibles al público, cuando sean de carácter económico, financiero, bancario o comercial, se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos,

dirección o fecha de nacimiento, o sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios.

Tampoco requerirá de esta autorización el tratamiento de datos personales que realicen personas jurídicas privadas para el uso exclusivo suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquéllos.

Al iniciarse el estudio de esta materia, se hizo presente que el proyecto de ley del Ejecutivo reemplaza esta disposición por la siguiente:

"Título I
De los derechos del titular de datos personales

Artículo 4º.- Derechos del titular de datos. Toda persona, actuando por sí o a través de su representante legal o mandatario, según corresponda, tiene derecho de acceso, rectificación, cancelación, oposición y portabilidad de sus datos personales, de conformidad a la presente ley.

Los derechos de acceso, rectificación, cancelación y oposición son personales, intransferibles e irrenunciables y no pueden limitarse por ningún acto o convención.

En caso de fallecimiento del titular de datos, los derechos que reconoce esta ley pueden ser ejercidos por sus herederos.".

Asimismo, la Comisión tuvo presente que la Moción parlamentaria que se refunde en esta iniciativa sugiere reemplazar este precepto por las siguientes disposiciones:

"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;

e) 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;

f) la posible cesión o transferencia internacional y su finalidad, cuando corresponda.

g) 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.”.

Al iniciarse el estudio de esta materia, el grupo de asesores parlamentarios sugirió a la Comisión aprobar el texto del artículo 4° presentado por el Ejecutivo.

Asimismo, **los representantes del Ejecutivo, señora Piedrabuena y señor Godoy**, explicaron que los derechos que no están incorporados en el artículo 4° se encuentran recogidos en otras disposiciones del proyecto.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena, recordó que el derecho de información contenido en el texto de la moción ya está consagrado como principio. Agregó que el derecho de acceso considera la obligación de informar. Finalmente, destacó que en la enumeración que realiza el artículo 4° propuesto por el Ejecutivo, se sigue el modelo de otras legislaciones.

El Presidente de la Comisión, Honorable Senador señor Harboe, consultó cuál es la razón de que en el inciso segundo del proyecto del Ejecutivo no se considere el derecho a la portabilidad.

El asesor del Ministerio de Hacienda, señor Godoy, explicó que el mencionado derecho es nuevo, está vinculado al mundo de *Internet* y genera costos tecnológicos y económicos cuando se ejerce. Agregó que no es un derecho irrenunciable.

El Presidente de la Comisión, Honorable Senador señor Harboe se mostró en desacuerdo con este planteamiento. Argumentó que se puede convertir en un derecho que no será ejercido. Sugirió que se emplee en el inciso segundo del texto propuesto por el Ejecutivo la expresión: “Tales derechos”, con el objeto de no excluir el derecho a la portabilidad.

El asesor del Comité Udi, señor Héctor Mery, mencionó que en el inciso primero se dice que: “Toda persona actuando por sí o a través de su representante legal o mandatario”, y en el segundo se señala: “Los derechos de acceso, rectificación, cancelación y oposición son personales…”. Preguntó si el uso del término “personales” quiere significar que no pueden ejercerse mediante representante.

El Presidente de la Comisión, Honorable Senador señor Harboe indicó que estos derechos sí pueden ser ejercidos por un representante.

Concluido el estudio de esta materia, **el señor Presidente de la Comisión** puso en votación el siguiente texto:

“Título I
De los derechos del titular de datos personales

Artículo 4º.- Derechos del titular de datos. Toda persona actuando por sí o a través de su representante legal o mandatario, según corresponda, tiene derecho de acceso, rectificación, cancelación, oposición y portabilidad de sus datos personales, de conformidad a la presente ley.

Tales derechos son personales, intransferibles e irrenunciables y no pueden limitarse por ningún acto o convención.

En caso de fallecimiento del titular de datos, los derechos que reconoce esta ley pueden ser ejercidos por sus herederos.”.

La Comisión, por la unanimidad de sus miembros presentes, los Honorables Senadores señores De Urresti, Harboe y Larraín, aprobó esta redacción.

Artículo 5º

A continuación, la Comisión examinó la regulación del derecho de acceso contenida en el proyecto de ley del Ejecutivo.

El artículo 5° vigente establece que el responsable de registro o banco de datos podrá establecer un procedimiento automatizado de transmisión de datos y los antecedentes de los que se deben dejar constancia cuando se transfieren datos.

En esta materia, el proyecto de ley del Ejecutivo, propone reemplazar dicha norma por la siguiente:

“Artículo 5.- Derecho de acceso. El titular de datos tiene derecho a solicitar y obtener del responsable confirmación acerca de si los datos personales que le conciernen están siendo tratados por él y, en tal caso, acceder a dichos datos y a la siguiente información:

a) Los datos tratados y su origen.

b) La finalidad o finalidades del tratamiento.

c) Las categorías, clases o tipos de destinatarios a los que se han comunicado o cedido los datos o se prevé comunicar o ceder, según corresponda.

d) El período de tiempo durante el cual los datos serán tratados.

El responsable no estará obligado a entregar al titular la información establecida en las letras anteriores cuando el titular ya disponga de esta información por haber ejercido este derecho con anterioridad; cuando su comunicación resulte imposible o requiera de un esfuerzo no razonable; cuando su entrega imposibilite u obstaculice gravemente un tratamiento de datos con fines históricos, estadísticos o científicos y para estudios o investigaciones que atiendan fines de interés público o vayan en beneficio de la salud humana; cuando los datos estén protegidos por una norma de secreto o una obligación de confidencialidad que impida su comunicación, o cuando lo disponga expresamente la ley.”.

Sobre esta materia, la Comisión tuvo presente que la Moción parlamentaria que se refunde en esta iniciativa propone lo siguiente:

“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.”.

Por su parte, el grupo de asesores parlamentarios sugirió a la Comisión, regular el derecho al acceso en los siguientes términos:

“Artículo 5.- Derecho de acceso. El titular de datos tiene derecho a solicitar y obtener del responsable, confirmación acerca de si los datos personales que le conciernen están siendo tratados por él, y en tal caso, acceder a dichos datos y a la siguiente información:

a) Los datos tratados y su origen;

b) La finalidad o finalidades del tratamiento;

c) Las categorías, clases o tipos de destinatarios a los que se han comunicado o cedido los datos o se prevé comunicar o ceder, según corresponda, y

d) El período de tiempo durante el cual los datos serán tratados.

El responsable no estará obligado a entregar al titular la información establecida en las letras anteriores cuando el titular ya disponga de esta información; cuando su comunicación resulte imposible o exija un esfuerzo desproporcionado; cuando su entrega imposibilite u obstaculice gravemente un tratamiento de datos con fines históricos, estadísticos o científicos y para estudios o investigaciones que atiendan fines de interés público o vayan en beneficio de la salud humana, o cuando lo disponga expresamente la ley.”.

Al iniciarse el estudio de esta materia, **el Presidente de la Comisión, Honorable Senador señor Harboe,** precisó que el texto de la Moción consideraba el acceso gratuito, y éste no se establece en el texto refundido.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena, afirmó que la gratuidad se encuentra consignada en una disposición posterior. Aclaró que la gratuidad del derecho de acceso se considera para un período determinado y siempre que no supere una cantidad que se indica.

El asesor del Honorable Senador señor Larraín, señor Olmedo, indicó que en el inciso final, específicamente en la primera excepción, que se refiere al caso en que el titular dispone de la información, no tendría motivo para ejercer el derecho de acceso.

Connotó que en la segunda hipótesis, cuando se señala: “cuando su comunicación resulte imposible o exija un esfuerzo desproporcionado”, solo resulta razonable establecer esta última como una verdadera excepción.

La asesora del Ministerio de Economía, señora Piedrabuena, comentó, respecto al primer problema planteado por el señor Olmedo, que un titular de datos bien intencionado no pedirá la información si dispone de ella. Pero alguien que no lo sea, puede establecer un algoritmo automático para solicitar reiteradamente información con la finalidad de bloquear el servidor. Subrayó que es importante mantener la excepción en cuestión.

En relación a la hipótesis que consiste en que la comunicación resulte imposible, se está pensando en bases de datos que no se conservaron en medios electrónicos, o que fueron guardados en cintas, o que se quemó un servidor. Todo ello imposibilita entregar la información.

El Presidente de la Comisión, Honorable Senador señor Harboe sugirió mejorar la redacción de la última parte del inciso final, ya que tal como está redactada puede dar a entender que luego del último (;), estaríamos en presencia de más de una hipótesis.

Propuso la siguiente redacción en el inciso final: “El responsable no estará obligado a entregar al titular, previa justificación, la información establecida…”

El asesor del Comité Udi, señor Mery consideró que es la Agencia de Protección de Datos la llamada a calificar la negativa del responsable.

El Honorable Senador, señor De Urresti solicitó que se definiera qué se entiende por esfuerzo desproporcionado. Preguntó en qué casos estamos en esa situación.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena, señaló que podía citar ciertos ejemplos, como el caso de la información que se guarda en un *diskette*; o los que se conservan en los archivos que tiene la Biblioteca Nacional.

El asesor del Ministerio de Hacienda, señor Godoy, precisó que la expresión también se encuentra recogida cuando se define dato personal, a saber, el artículo 2°, letra f) del proyecto.

El Honorable Senador señor Larraín propuso un mayor orden en la redacción del inciso final, y que las hipótesis de excepción se enumeren.

A partir de estos planteamientos los representantes del Ejecutivo sugirieron a la Comisión aprobar el artículo 5°, en los siguientes términos:

“Artículo 5º.- Derecho de acceso. El titular de datos tiene derecho a solicitar y obtener del responsable, confirmación acerca de si los datos personales que le conciernen están siendo tratados por él, y en tal caso, acceder a dichos datos y a la siguiente información:

a) Los datos tratados y su origen;

b) La finalidad o finalidades del tratamiento;

c) Las categorías, clases o tipos de destinatarios a los que se han comunicado o cedido los datos o se prevé comunicar o ceder, según corresponda, y

d) El período de tiempo durante el cual los datos serán tratados.

El responsable no estará obligado a entregar la información solicitada por el titular en los siguientes casos:

i. Cuando el titular ya disponga de la información requerida;

ii. Cuando su comunicación resulte imposible o su entrega exija un esfuerzo desproporcionado;

iii. Cuando su entrega imposibilite u obstaculice gravemente un tratamiento de datos con fines históricos, estadísticos o científicos, para estudios o investigaciones que atiendan fines de interés público o vayan en beneficio de la salud humana, y

iv. Cuando lo disponga expresamente la ley.”.

El Presidente de la Comisión, Honorable Senador señor Harboe observó que si a un titular de datos se le niega la

información, podrá reclamar de acuerdo al procedimiento que se regula más adelante en esta ley.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó esta redacción.

Artículo 6º

A continuación, la Comisión examinó el artículo 6º contenido en el proyecto de ley que presentó el Ejecutivo, disposición que regula el derecho a rectificación.

Al iniciarse su estudio, la Comisión tuvo presente lo estatuido en el artículo 6º de la ley Nº 19.628, sobre protección de la Vida Privada.

La norma vigente prescribe que los datos personales deberán ser eliminados o cancelados cuando su almacenamiento carezca de fundamento legal o cuando hayan caducado.

Agrega que deben ser modificados cuando sean erróneos, inexactos, equívocos o incompletos.

Precisa que se bloquearán los datos personales cuya exactitud no pueda ser establecida o cuya vigencia sea dudosa y respecto de los cuales no corresponda la cancelación.

Concluye que el responsable del banco de datos personales procederá a la eliminación, modificación o bloqueo de los datos, en su caso, sin necesidad de requerimiento del titular.

El proyecto de ley del Ejecutivo sustituye este precepto por el siguiente:

“Artículo 6.- Derecho de rectificación. El titular de datos tiene derecho a solicitar y obtener del responsable la rectificación de los datos personales que le conciernen y que están siendo tratados por él, cuando sean inexactos, desactualizados o incompletos.

La rectificación y su contenido serán públicas y deberán difundirse cuando así lo requiera el titular y sea necesario para los fines del tratamiento realizado.”.

Asimismo, la Comisión tuvo presente que esta materia está regulada en el artículo 14 de la Moción parlamentaria que se refunde en esta iniciativa. Este precepto dispone lo siguiente:

"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.".

Al iniciarse el estudio de esta materia, el grupo de asesores parlamentarios sugirió a la Comisión aprobar el texto propuesto por el Ejecutivo.

El Presidente de la Comisión, Honorable Senador señor Harboe destacó que en el texto de la Moción se utiliza la expresión "innecesarios". Destacó que se justifica su eliminación, porque en el principio de calidad se indica que los datos personales deben ser exactos, completos y actuales, en relación con los fines del tratamiento.

La asesora del Ministerio de Economía, **señora Piedrabuena,** aseveró que en el caso que los datos sean innecesarios puede proceder el derecho a cancelación.

Concluido el debate sobre este asunto, el señor Presidente de la Comisión puso en votación este precepto.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores De Urresti, Harboe y Larraín, aprobó el artículo 6º propuesto por el Ejecutivo.

Artículo 7º

En seguida, la Comisión consideró la sustitución del artículo 7º de la ley Nº 19.628.

La norma vigente prescribe 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, obligación que no cesa por haber terminado sus actividades en ese campo.

El proyecto de ley del Ejecutivo propone aprobar un nuevo artículo 7º que regula el derecho de cancelación. Su texto es el siguiente:

“Artículo 7.- Derecho de cancelación. El titular de datos tiene derecho a solicitar y obtener del responsable la cancelación o supresión de los datos personales que le conciernen cuando éstos no resulten necesarios en relación con los fines del tratamiento; cuando haya retirado su consentimiento para el tratamiento y éste no tenga otro fundamento legal; cuando se trate de datos caducos; cuando los datos hayan sido obtenidos o tratados ilícitamente por el responsable o cuando la cancelación deba realizarse para el cumplimiento de una obligación legal.

Sin perjuicio de lo anterior, no procede la cancelación o supresión de los datos en los siguientes casos:

a) Cuando el tratamiento sea necesario para ejercer el derecho a las libertades de emitir opinión y de informar regulado por las leyes a que se refiere el artículo 19 N° 12 de la Constitución Política de la República.

b) Cuando se requiera el tratamiento de los datos para el cumplimiento de una obligación legal o la ejecución de un contrato del que el titular es parte.

c) Cuando existan razones de interés público en el ámbito de la salud pública.

d) Cuando el tratamiento se realice con fines históricos, estadísticos o científicos y para estudios o investigaciones que atiendan fines de interés público, en la medida que la cancelación de los datos imposibilite u obstaculice gravemente el propósito de este tratamiento.

e) Cuando se requieran para la formulación, ejercicio o defensa de una reclamación formulada en el marco de esta ley.”.

En relación a esta materia, la Moción parlamentaria también regula el derecho a cancelación en su artículo 15. En este precepto se dispone lo siguiente:

“Articulo 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.”.

Al comenzar el estudio de esta modificación, el grupo de asesores parlamentarios sugirió a la Comisión aprobar el proyecto del Ejecutivo enmendado en los siguientes términos:

“Artículo 7.- Derecho de cancelación. El titular de datos tiene derecho a solicitar y obtener del responsable, la cancelación o supresión de los datos personales que le conciernen, cuando éstos no resulten necesarios en relación con los fines del tratamiento para el cual fueron recogidos; cuando haya retirado su consentimiento para el tratamiento y éste no tenga otro fundamento legal, o cuando los datos hayan sido obtenidos o tratados ilícitamente por el responsable.

Sin perjuicio de lo anterior, no procede la cancelación de los datos en los siguientes casos:

a) Cuando el tratamiento sea necesario para ejercer el derecho a las libertades de emitir opinión y de informar, regulado en el artículo 19 N° 12 de la Constitución Política de la República.

b) Cuando se requiera el tratamiento de los datos para el cumplimiento de una obligación legal o la ejecución de un contrato.

c) Cuando existan razones de interés público, especialmente en el ámbito de la salud pública.

d) Cuando el tratamiento de los datos se realice con fines históricos, estadísticos o científicos y para estudios o investigaciones que atiendan fines de interés público.

e) Cuando los datos se requieran para la formulación, ejercicio o defensa de una reclamación formulada en el marco de esta ley.”.

El Presidente de la Comisión, Honorable Senador señor Harboe observó que las normas europeas han contemplado el derecho de los ciudadanos a pedir la cancelación de determinado tipo de información almacenada en sus páginas *web*. Preguntó por qué en la presente iniciativa se excluye dicha posibilidad.

El asesor del Ministerio de Hacienda, señor Godoy precisó que en el artículo 1° se estableció un límite que consistía en que la protección de la privacidad de las personas y los demás derechos fundamentales vinculados al resguardo de la información pueden entrar en colisión con otros derechos fundamentales, y uno de esos conflictos, eventualmente, puede producirse con la libertad de información y la de opinión. Añadió que de acuerdo a la normativa actual, que regula la legislación en materia de protección de datos y que se recoge en el texto propuesto por el grupo de asesores, se mantiene el límite antes mencionado, que consiste en que frente a un conflicto eventual de derechos, la libertad de opinión e información tendrán preferencia frente al derecho a la protección de la información de las personas.

El asesor del Comité Udi, señor Mery sostuvo que no se puede entender el derecho de cancelación como un derecho absoluto. Destacó que estamos ante cuestiones que se irán a dilucidar en la práctica y tendrán que resolverse de acuerdo a los principios de la presente ley.

Llamó la atención que en la letra a) de la redacción propuesta se haga referencia a la emisión de opinión e información en los términos regulados en el artículo 19 N° 12 de la Constitución Política de la República, puesto que la densidad regulatoria y el contenido esencial de ese derecho es más amplio que el tratado en el referido artículo. Puntualizó que si se analiza el artículo 1° de la ley N° 19.733 se habla de cuestiones que escapan al derecho regulado en la Constitución y, por lo mismo, es más completa.

El Presidente de la Comisión, Honorable Senador señor Harboe, sostuvo que el derecho de cancelación constituye una expresión del derecho al olvido. Consignó que este último ha ido ganando espacio en la doctrina y en la jurisprudencia internacional, particularmente en aquellos casos donde hay cierta información que afecta derechos fundamentales y la privacidad de las personas como, por ejemplo, cuando se publica algo manifiestamente falso. Surge en ese caso el legítimo derecho de exigir del medio de comunicación, o de la plataforma en la cual está publicada, la eliminación de esa información.

El asesor del Honorable Senador señor Larraín, **señor Olmedo,** constató que hoy en día la situación descrita se resuelve vía recurso de protección. Consideró que la Agencia de Protección de Datos podrá no estar dotada de la capacidad suficiente para hacerse cargo de las situaciones planteadas.

El Presidente de la Comisión, Honorable Senador señor Harboe, reiteró que los tribunales de justicia se han hecho cargo de lo planteado. Subrayó que éstos deberán resolver los casos que se le presentan aplicando esta ley. Por lo mismo, argumentó, se debe consagrar el derecho al olvido.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena, hizo presente que no es la plataforma electrónica la que emite la opinión, sino que es el periódico, o el blog, etcétera.

El asesor del Ministerio de Hacienda, señor Godoy, precisó que la excepción que se establece es que frente al derecho de las personas a resguardar su información personal, ella cede ante la libertad de emitir opinión e información. Sin embargo, ello no significa que las últimas dos libertades mencionadas sean derechos absolutos y que no tengan regulación particular.

El Presidente de la Comisión, Honorable Senador señor Harboe, acotó que el legislador debe hacerse cargo de las nuevas realidades, como por ejemplo, el auge de las redes sociales y la impunidad que existe para difundir noticias falas en esas plataformas. Precisó que resulta aún más grave que a través de buscadores se indexe la información a determinados nombres e instituciones y que esto termine publicándose. Ello genera una afectación de los derechos fundamentales.

Consultó cómo se compatibiliza y se logra evitar una afectación de otros derechos, tales como, el de privacidad, honra, dignidad. Por lo anterior, pidió a los representantes del Ejecutivo mejorar la redacción de este precepto.

En una sesión posterior, el Ejecutivo sugirió a la Comisión aprobar la siguiente redacción alternativa:

“Artículo 7.- Derecho de cancelación. El titular de datos tiene derecho a solicitar y obtener del responsable la cancelación o supresión de los datos personales que le conciernen, en los siguientes casos.

a) Cuando los datos no resulten necesarios en relación con los fines del tratamiento para el cual fueron recogidos;

b) Cuando el titular haya revocado su consentimiento para el tratamiento y éste no tenga otro fundamento legal;

c) Cuando los datos hayan sido obtenidos o tratados ilícitamente por el responsable;

d) Cuando se trate de datos caducos;

e) Cuando los datos deban suprimirse para el cumplimiento de una sentencia judicial o de una obligación legal, y

f) Cuando el titular haya ejercido su derecho de oposición de conformidad al artículo siguiente y no existan otro fundamento legal para su tratamiento.

No procede la cancelación cuando el tratamiento sea necesario:

i. Para ejercer el derecho a las libertades de emitir opinión y de informar;

ii. Para el cumplimiento de una obligación legal o la ejecución de un contrato suscrito entre el titular y el responsable;

iii. Por razones de interés público, especialmente en el ámbito de la salud pública;

iv. Para tratamientos con fines históricos, estadísticos o científicos y para estudios o investigaciones que atiendan fines de interés público, y

v. Para la formulación, ejercicio o defensa de una reclamación administrativa o judicial.”.

Luego de la lectura de esta proposición, **la Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó esta última redacción.**

Artículo 8º

En una sesión posterior, la Comisión consideró una enmienda al artículo 8º de la ley Nº 19.628.

Actualmente este precepto establece que en el caso de que el tratamiento de datos personales se efectúe por mandato, se aplicarán las reglas generales.

El mandato deberá ser otorgado por escrito, dejando especial constancia de las condiciones de la utilización de los datos.

El mandatario deberá respetar esas estipulaciones en el cumplimiento.

El proyecto de ley del Ejecutivo sustituye esta disposición por otra que regula el derecho de oposición. Su texto es el siguiente:

“Artículo 8°.- Derecho de oposición. El titular de datos tiene derecho a oponerse ante el responsable a que se realice un tratamiento específico o determinado de los datos personales que le conciernan, en los siguientes casos:

a) Cuando el tratamiento de datos afecte sus derechos y libertades fundamentales.

b) Cuando el tratamiento de datos sea utilizado exclusivamente con fines de marketing directo de bienes o servicios, así como cualquier otro propósito comercial o fines publicitarios, salvo que exista un contrato entre las partes que expresamente contemple dicho uso de su información.

c) Cuando se realice tratamiento automatizado de sus datos personales y se adopten decisiones que impliquen una valoración, evaluación o predicción de su comportamiento realizada únicamente en base a este tipo de tratamiento, salvo las excepciones previstas en el artículo 15 ter de esta ley.

d) Cuando el titular de los datos hubiere fallecido. En este caso, la oposición deberá ser formulada por los herederos. Con todo, no procederá la oposición cuando el tratamiento de los datos se realice exclusivamente con fines históricos, estadísticos o científicos o para estudios o investigaciones que atiendan fines de interés público.”

En relación a esta materia, la moción parlamentaria que se refunde en este proyecto propone regular el derecho de oposición en su artículo 16, precepto que prescribe lo siguiente:

“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.

e) Los datos sean usados para la elaboración de perfiles.”.

Al iniciarse el estudio de estas modificaciones, el grupo de asesores parlamentarios, propuso a la Comisión aprobar el texto del proyecto del Ejecutivo, enmendado en la siguiente forma:

“Artículo 8.- Derecho de Oposición. El titular de datos tiene derecho a oponerse ante el responsable a que se realice un tratamiento específico o determinado de los datos personales que le conciernan, en los siguientes casos:

a) Si el tratamiento afecta sus derechos y libertades fundamentales.

b) Si el tratamiento está referido a datos caducos.

c) Si el tratamiento se realiza exclusivamente con fines de mercadotecnia o marketing directo de bienes, productos o servicios, salvo que exista un contrato entre las partes.

d) Si se realice tratamiento automatizado de sus datos personales para la elaboración de perfiles que impliquen una valoración, evaluación o predicción de su comportamiento, realizada únicamente en base a este tipo de tratamiento y se adopten decisiones que le afecten significativamente en forma negativa, salvo que el tratamiento sea necesario para la celebración o ejecución de un contrato entre el titular y el responsable y exista consentimiento previo y expreso del titular, o lo disponga la ley.

e) Si el titular de los datos hubiere fallecido. En este caso, la oposición deberá ser formulada por los herederos.

f) Si el tratamiento se realiza en base a datos obtenidos de una fuente de acceso público.

No obstante, la oposición no procederá en los siguientes casos:

i. Cuando el tratamiento sea necesario para ejercer el derecho a las libertades de emitir opinión y de informar regulado por las leyes a que se refiere en el artículo 19 N° 12 de la Constitución Política de la República.

ii. Cuando existan razones de interés público.

iii. Cuando el tratamiento de los datos se realice con fines históricos, estadísticos o científicos y para estudios o investigaciones que atiendan fines de interés público.

iv. Cuando el tratamiento se requiera para la formulación, ejercicio o defensa de una reclamación formulada en el marco de esta ley.”.

L**a asesora del Ministerio de Economía, señora Bernardita Piedrabuena,** explicó que el derecho de oposición es aquel que se ejerce para impedir el tratamiento de un dato específico. Es decir, no se elimina el dato, pero se bloquea en la base respectiva.

Agregó que las causales para invocarlo replican, en lo sustancial, aquellas que se establecen en la Moción.

Destacó que la diferencia fundamental entre el derecho de oposición y cancelación se manifiesta en la forma en que se ejerce. El primero de ellos se manifiesta cuando la fuente de licitud no emana del consentimiento. Por el contrario, el de cancelación se ejerce cuando la fuente de legitimidad es el consentimiento.

El Presidente de la Comisión, Honorable Senador, señor Felipe Harboe expresó que si nos atenemos a la diferencia conceptual entre el derecho de cancelación y de oposición, podría ocurrir que en aquellos casos en que no medie consentimiento y la fuente sea distinta, habría que ejercer el derecho de oposición. Añadió que la consecuencia de ésta, es la cancelación.

Sostuvo que si una persona solicita la cancelación respecto de un dato cuya fuente no ha sido el consentimiento, alguien podría negarse, porque la fuente no emanaría del consentimiento. Preguntó cómo se resuelve la situación descrita.

El Honorable Senador, señor Larraín indicó que procede la cancelación cuando la fuente de licitud del tratamiento proviene del consentimiento.

Seguidamente, planteó una duda respecto al caso que regula la letra e), disposición que señala lo siguiente:

“e) Si el titular de los datos hubiere fallecido. En este caso, la oposición deberá ser formulada por los herederos.”.

Recalcó que en la hipótesis transcrita, hubo consentimiento del titular. El hecho del fallecimiento abre un escenario distinto, a saber, que el consentimiento no lo prestaron los herederos. Subrayó que desde el punto de vista jurídico los herederos son los continuadores jurídicos y patrimoniales del causante. Por lo tanto, respecto a los sucesores no debería haber oposición, sino que cancelación.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena, manifestó que en el artículo 7° se establecen los casos en que opera la cancelación, y éstos son, entre otros, cuando los datos no resulten necesarios para los fines para los cuales fueron recogidos. Lo anterior se puede presentar en un caso de consentimiento, pero también en uno de fuente de acceso público.

El Presidente de la Comisión, Honorable Senador señor Felipe Harboe, aseveró que hay un conjunto de datos donde no media el consentimiento, por ejemplo, aquellos que estén en poder del Servicio de Salud. Agregó que el fin de esos datos responde a un tema sanitario. Si, por ejemplo, esos datos se ocuparan para enviar publicidad, un individuo se podría oponer a que se utilice esa base de datos y pedir que se cancele su uso no autorizado.

El asesor del Ministerio de Hacienda, señor Godoy, puntualizó que efectivamente no hay una nitidez absoluta al hacer la distinción entre el derecho de cancelación y el de oposición. Toda la sistemática de las legislaciones termina estableciendo causales en uno y otro caso.

Destacó que la diferencia entre ellos se encuentra fundamentalmente en la fuente de legitimidad. Agregó que el consentimiento, como fuente, no es exclusivo del derecho de cancelación.

Señaló que la diferencia principal tiene que ver con el efecto del ejercicio de un derecho y otro. Añadió que en el ejercicio del derecho de cancelación el efecto que se produce es que el dato es

suprimido. En el derecho de oposición, éste no se elimina, sino que no se realiza el tratamiento.

Hizo presente que aquellas hipótesis que el Ejecutivo definió como propuestas de cancelación, son aquellas en que no existe fundamento para efectuar ese tratamiento. Sostuvo que en caso de dato caduco, puede ser necesario que éstos no sean tratados, pero que no sean eliminados. Ejemplificó con el caso del Servel, que si bien posee un historial de los domicilios anteriores de una persona, el dato relevante es el domicilio actual.

El Presidente de la Comisión, Honorable Senador señor Felipe Harboe, advirtió que en estas normas se les está confiriendo derechos a los titulares. Por lo tanto, si un titular se opone a que una determinada base de datos, sea pública o privada, tenga domicilios anteriores, por innecesarios, debe poder ejercer el derecho a cancelación.

Finalmente, recordó que puede ocurrir que la utilización de datos caducos tenga consecuencias negativas a los titulares de datos.

El asesor del Ministerio de Hacienda, señor Godoy, declaró que si un dato actualizado no es necesario para los fines del tratamiento, el derecho que surge es el de la cancelación.

El Presidente de la Comisión, Honorable Senador señor Harboe, connotó que si un dato actualizado no es de interés se puede pedir la cancelación. Preguntó qué justificación hay para almacenar un dato caduco.

Agregó que en el derecho comparado se establece que la caducidad da derecho a la cancelación, sea en 5, 7, 8 o 10 años, según el país de que se trate. Se preguntó por qué en Chile no se puede consagrar la cancelación, tal como se hace en otras legislaciones.

El Honorable Senador señor Larraín inquirió por cuál sería el problema de mantener como causal de cancelación los datos caducos.

El asesor del Ministerio de Hacienda, señor Godoy adujo que el efecto de la cancelación es la supresión del dato. Por lo tanto, se elimina del registro. Acotó que existirán algunos tratamientos en que suprimir un dato puede acarrear consecuencias que uno no necesariamente prevé en el momento en que el titular ejerce ese derecho.

El Presidente de la Comisión, Honorable Senador señor Harboe, expresó que hay hipótesis en las cuales se niega el derecho de cancelación. Aseveró que éste no es absoluto.

Atendido lo anterior, consideró que la letra b) del artículo 8° se debe mantener en el artículo 7°.

Respondiendo a la pregunta del Honorable Senador señor Larraín, respecto a la letra e), **la asesora del Ministerio de Economía, señora Bernardita Piedrabuena,** enfatizó que hubo una larga discusión sobre este tema en el grupo de asesores parlamentarios. En esa instancia, se analizó si el consentimiento constituía una acción personalísima. La pregunta que surge es si el consentimiento que otorgó el titular se transmite a sus herederos. Constató que en el caso planteado, surge el derecho de los sucesores a oponerse.

El Honorable Senador señor Larraín hizo presente que el consentimiento lo otorgó el titular y si éste fallece no puede entenderse que la manifestación de voluntad se suspende. Estimó conveniente que el caso planteado se consagre, pero dentro del derecho de cancelación, y no en el de oposición.

El asesor del Ministerio de Hacienda, señor Godoy, expresó que como la fuente de legitimidad en el caso del consentimiento es la voluntad del titular, al haber fallecido, éste no está en condiciones de poder retirar su consentimiento. Agregó que los herederos constituyen una persona distinta del titular de datos. Dado lo anterior, explicó que consideraron más pertinente incorporarlo dentro del derecho de oposición.

El Presidente de la Comisión, Honorable Senador señor Harboe, consignó que la diferencia conceptual entre ambos derechos no es tan nítida. Acotó que se puede pedir la cancelación de datos que no se han almacenado en virtud del consentimiento.

Remarcó que no es tan fácil de separar el dato que se origina en el consentimiento del resto de las fuentes.

El Honorable Senador señor Larraín consideró relevante establecer una diferencia, de lo contrario no existe justificación para mantener separados ambos derechos.

El Presidente de la Comisión, Honorable Senador señor Harboe, indicó que hay dos momentos. Ejemplificó con el caso de una persona que ingresa a un edificio y le piden sus datos, surge ahí el derecho de oposición. Otro momento posterior se produce cuando los

datos de ese individuo ya se encuentran almacenados. En esa última situación emana el derecho a que éstos se cancelen.

Precisó que la diferencia entre ambos derechos no proviene solo de la fuente, sino que también del momento en que se pueden ejercer.

La asesora del Ministerio de Economía, señora Piedrabuena, reconoció que la línea divisoria entre los derechos mencionados no es tan clara.

El Presidente de la Comisión, Honorable Senador señor Harboe, consultó cómo lo resuelve el derecho comparado.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena, manifestó que en el Reglamento de la Comunidad Europea se tratan conjuntamente, pero los denomina: de supresión y de oposición.

El Presidente de la Comisión, Honorable Senador señor Harboe, aseveró que se podría considerar el derecho de cancelación y de oposición conjuntamente.

La asesora del Ministerio de Economía, señora Piedrabuena, subrayó que en la legislación de Latinoamérica, y en las normas de la OCDE y de la APEC, se tratan separadamente.

El Presidente de la Comisión, Honorable Senador señor Harboe consignó que si así se tratan, debe existir un fundamento para ello.

Seguidamente, **la asesora del Ministerio de Economía, la señora Piedrabuena** hizo referencia a las normas de la Unión Europea. En ellas no se contempla el caso de que el titular de un dato fallezca.

El asesor del Ministerio de Hacienda, señor Godoy, hizo presente que se acaba de publicar la nueva ley argentina en materia de protección de datos, y ella distingue entre el derecho de oposición y de supresión, ambas con causales específicas.

Reseñó que algunas causales de supresión son las siguientes:

- Los datos personales ya no son necesarios en relación con los fines para el tratamiento;

- Cuando el titular de datos revoca el consentimiento;

- Cuando el titular de datos haya ejercido su derecho a oposición;

- Los datos personales hayan sido tratados ilícitamente.

El Presidente de la Comisión, Honorable Senador señor Harboe llamó la atención respecto a la causal que señala: “Cuando el titular de datos haya ejercido su derecho a oposición”. Indicó que puede ocurrir que alguien ejerza su derecho a oposición y, además, solicite la cancelación.

Constató que debe haber una norma de conexión entre ambos derechos.

Sugirió que el Ejecutivo estudie una nueva redacción para esta norma. Asimismo, pidió que se revise especialmente el texto de la letra d).

Hizo referencia a la letra d), del artículo 16 de la Moción, que señala:

“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:

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.”

Consignó que en la Cámara de Diputados se está discutiendo la iniciativa que modifica las leyes N°s 19.496 y 19.628, para regular la protección de la vida privada en lo relativo al envío de publicidad (Boletín 10.133-03). En ella se establece un mecanismo de prohibición de envío de publicidad. Dado lo anterior, consideró relevante recoger la norma antes transcrita.

La asesora del Ministerio de Economía, señora Piedrabuena, reconoció que los miembros de la Comisión de Economía de la Cámara Baja, no son partidarios de que una persona se tenga que registrar en una lista para evitar el envío de publicidad. Se manifestaron de acuerdo con la libertad de envío, pero con la posibilidad de oponerse.

En una sesión posterior, **los representantes del Ejecutivo, señora Piedrabuena y señor Godoy**, propusieron a la Comisión aprobar el siguiente artículo 8°:

“Artículo 8.- Derecho de Oposición. El titular de datos tiene derecho a oponerse ante el responsable a que se realice un tratamiento específico o determinado de los datos personales que le conciernan, en los siguientes casos:

a) Si el tratamiento afecta sus derechos y libertades fundamentales;

b) Si el tratamiento se realiza exclusivamente con fines de mercadotecnia o *marketing* directo de bienes, productos o servicios, salvo que exista un contrato entre el titular y el responsable;

c) Si el titular de los datos hubiere fallecido. En este caso, la oposición deberá ser formulada por los herederos, y

d) Si el tratamiento se realiza respecto de datos obtenidos de una fuente de acceso público y no exista otro fundamento legal para su tratamiento.

No procederá la oposición al tratamiento en los siguientes casos:

i. Cuando sea necesario para ejercer el derecho a las libertades de emitir opinión y de informar;

ii. Cuando existan razones de interés público, especialmente en el ámbito de la salud pública;

iii. Cuando se realice con fines históricos, estadísticos o científicos y para estudios o investigaciones que atiendan fines de interés público, y

iv. Cuando se requiera para la formulación, ejercicio o defensa de una reclamación administrativa o judicial.”.

Luego de la lectura de esta redacción, **la Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó esta disposición.**

Artículo 8° bis

A continuación, los mencionados representantes del Ejecutivo sugirieron a la Comisión aprobar un **artículo 8º bis**, nuevo, que consagra el derecho de oposición a valoraciones personales automatizadas.

La norma propuesta dispone lo siguiente:

“Artículo 8 bis.- Derecho de oposición a valoraciones personales automatizadas. El titular de datos tiene derecho a oponerse a que el responsable adopte decisiones que le afecten significativamente en forma negativa o le produzcan efectos jurídicos adversos, basadas únicamente en el tratamiento automatizado de sus datos personales, incluida la elaboración de perfiles.

El titular no podrá ejercer este derecho de oposición en los siguientes casos:

a) Cuando la decisión del responsable sea necesaria para la celebración o ejecución de un contrato entre el titular y el responsable;

b) Cuando exista consentimiento previo y expreso del titular, y

c) Cuando lo disponga la ley.

En los casos de las letras a) y b) del inicio anterior, el responsable deberá adoptar las medidas necesarias para asegurar los derechos del titular, en particular el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a solicitar la revisión de la decisión.”.

Al iniciarse su análisis, **el Presidente de la Comisión, Honorable Senador señor Harboe,** explicó que estamos ante la situación en que se introduce un conjunto de información respecto a una persona determinada en relación a sus comportamientos, y a través de un sistema de algoritmos se establece un perfil. Agregó que frente a un reclamo de quien ha sido objeto de dicho sistema, no existen normas que le permitan al ciudadano oponerse.

Consultó por el origen de esta disposición.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena, mencionó que ella obedece a la fusión de dos artículos, a saber, la letra d), del artículo 8º y el 15 ter. Recalcó que similar redacción está presente en la legislación argentina y europea.

Aclarado este punto, **el Presidente de la Comisión, Honorable Senador señor Harboe,** declaró clausurado el debate.

Seguidamente, **la Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó esta disposición.**

Artículo 9º

Mediante este precepto se modifica el artículo 9º de la ley Nº 19.628, sobre protección de la vida privada. Esta disposición prescribe 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.

Agrega que en todo caso, la información debe ser exacta, actualizada y responder con veracidad a la situación real del titular de los datos.

Adicionalmente, prohíbe la realización de todo tipo de predicciones o evaluaciones de riesgo comercial que no estén basadas únicamente en información objetiva relativa a las morosidades o protestos de las personas naturales o jurídicas de las cuales se informa. La infracción a esta prohibición obligará a la eliminación inmediata de dicha información por parte del responsable de la base de datos y dará lugar a la indemnización de perjuicios que corresponda.

El proyecto de ley del Ejecutivo reemplaza este artículo por otro que establece el derecho a la portabilidad de los datos personales. Su texto es el siguiente:

“Artículo 9º.- Derecho a la portabilidad de los datos personales. El titular de datos tiene derecho a solicitar y recibir del responsable una copia de los datos personales que le conciernen de manera estructurada, en un formato genérico y de uso común que permita ser operado por distintos sistemas, y a comunicarlos o transferirlos a otro responsable de datos, cuando concurran las siguientes circunstancias o requisitos:

a) El titular haya entregado sus datos personales directamente al responsable.

b) Se trate de un volumen relevante de datos y sean tratados en forma automatizada.

c) Exista consentimiento del titular para el tratamiento o se requiera para la ejecución o cumplimiento de un contrato.

El responsable debe utilizar los medios más expeditos, menos onerosos y sin poner trabas u obstáculos para el ejercicio de este derecho.

El responsable también debe comunicar al titular de manera clara y precisa las medidas necesarias para recuperar sus datos personales y especificar las características técnicas para llevar a cabo estas operaciones.”.

Por su parte, la moción parlamentaria, en su artículo 19, regula esta materia en los siguientes términos:

“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.”.

Al iniciarse el estudio de estas propuestas, el grupo de asesores parlamentarios sugirió a la Comisión aprobar el texto del proyecto de ley del Ejecutivo, enmendado en los siguientes términos:

“Artículo 9°.- Derecho a la portabilidad de los datos personales. El titular de datos tiene derecho a solicitar y recibir del responsable, una copia de los datos personales que le conciernen de manera estructurada, en un formato genérico y de uso común, que permita ser operado por distintos sistemas y, a comunicarlos o transferirlos a otro responsable de datos, cuando concurran las siguientes circunstancias o requisitos:

a) El titular haya entregado sus datos personales directamente al responsable. No procede el ejercicio de este derecho

respecto de la información inferida, derivada, creada, generada u obtenida a partir del análisis o tratamientos realizados por el responsable;

b) Se trate de un volumen relevante de datos y sean tratados en forma automatizada, y

c) Exista consentimiento del titular para el tratamiento o se requiera para la ejecución o cumplimiento de un contrato.

El responsable debe utilizar los medios más expeditos, menos onerosos y sin poner trabas u obstáculos para el ejercicio de este derecho.

El responsable también debe comunicar al titular de manera clara y precisa las medidas necesarias para recuperar sus datos personales y especificar las características técnicas para llevar a cabo estas operaciones.”.

Sobre esta propuesta, **el Presidente de la Comisión, Honorable Senador señor Harboe,** hizo referencia al primer requisito, que señala que: “El titular haya entregado sus datos personales directamente al responsable...”. Constató que no estamos ante un tratamiento ilegal. Por lo tanto, el individuo no tendrá derecho a pedir a una base de datos mal constituida, sin fuente legítima, que le entregue los datos.

La asesora del Ministerio de Economía, señora Piedrabuena, aseveró que esa base no debería existir. Agregó que si se están tratando datos sin fundamento legal, el infractor se arriesga a una sanción grave.

El Presidente de la Comisión, Honorable Senador señor Harboe, afirmó que se necesita un sistema que incentive la formalización del tratamiento de bases de datos.

El Honorable Senador, señor Araya solicitó se precise qué se entenderá por “volumen relevante de datos”.

El Honorable Senador señor Larraín hizo presente que en la letra a), se establece que el titular haya entregado sus datos y en la c), que exista consentimiento del titular para el tratamiento. Consultó si existe una diferencia entre ambas disposiciones

La asesora del Ministerio de Economía, señora Piedrabuena, respecto a la última pregunta, advirtió que existe un ejemplo en que ambas letras no se relacionan. Se refirió al caso de los organismos públicos que tratan datos por ley, y en la entrega de éstos no hay

consentimiento y la fuente de legitimidad es la ley. Subrayó que en el caso planteado no se ejerce el derecho de portabilidad.

En relación a la consulta del Honorable Senador señor Araya, precisó que, por ejemplo, en el *big data* se reúnen volúmenes relevantes de datos que se tratan en forma automatizada. Advirtió que el mencionado concepto dependerá de la tecnología y de las definiciones que realice la Agencia.

Concluido el análisis de estas disposiciones, el señor Presidente de la Comisión puso en votación el artículo 9º, con las enmiendas sugeridas por el grupo de asesores parlamentarios.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó esta disposición.

Artículo 10

Este precepto sustituye el artículo 10 de la ley N° 19.628, disposición que señala que no pueden ser objeto de tratamiento los datos sensibles, salvo cuando la ley lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares.

Esta disposición es reemplazada por otra que regula la forma y medios de ejercer los derechos del titular de datos.

El proyecto de ley del Ejecutivo propone la siguiente disposición:

“Artículo 10.- Forma y medios de ejercer los derechos del titular de datos. Los derechos reconocidos en esta ley se ejercen por el titular, en forma personal o debidamente representado, ante el responsable de datos. Si los datos personales del titular se encuentran en una base de datos que es administrada o tratada por diversos responsables, el titular puede ejercer sus derechos ante cualquiera de ellos.

Los responsables de datos deben implementar mecanismos y herramientas tecnológicas que permitan que el titular ejerza sus derechos en forma expedita, ágil y eficaz. Los medios dispuestos por el responsable deben ser sencillos en su operación.

El ejercicio de los derechos de rectificación, cancelación y oposición siempre serán gratuitos para el titular. El derecho de acceso también se ejercerá en forma gratuita, al menos, trimestralmente.

El responsable de datos sólo puede exigir el pago de los costos directos en que incurra cuando el titular ejerza su derecho de acceso más de una vez en el trimestre o cuando ejerza el derecho a la portabilidad.

La Agencia de Protección de Datos Personales deberá velar por el efectivo ejercicio y cumplimiento de los derechos que esta ley reconoce al titular.”.

Al iniciarse el estudio de esta disposición los representantes del Ejecutivo propusieron una indicación que agrega nuevos antecedentes referidos a la participación en esta materia de la Agencia de Protección de Datos. Su texto es el siguiente:

“Artículo 10.- Forma y medios de ejercer los derechos del titular de datos. Los derechos reconocidos en esta ley se ejercen por el titular ante el responsable de datos. Si los datos personales del titular son tratados por diversos responsables, el titular puede ejercer sus derechos ante cualquiera de ellos.

Los responsables de datos deberán implementar mecanismos y herramientas tecnológicas que permitan que el titular ejerza sus derechos en forma expedita, ágil y eficaz. Los medios dispuestos por el responsable deben ser sencillos en su operación.

El ejercicio de los derechos de rectificación, cancelación y oposición siempre serán gratuitos para el titular. El derecho de acceso también se ejercerá en forma gratuita, al menos trimestralmente.

El responsable de datos sólo puede exigir el pago de los costos directos en que incurra, cuando el titular ejerza su derecho de acceso más de una vez en el trimestre o cuando ejerza el derecho a la portabilidad.

La Agencia de Protección de Datos Personales a través de una norma de carácter general establecerá los parámetros y mecanismos para determinar los costos indicados en el inciso anterior.

La Agencia de Protección de Datos Personales velará por el efectivo ejercicio y cumplimiento de los derechos que esta ley reconoce al titular de datos.”.

Los integrantes de la Comisión valoraron este precepto dado que regula adecuadamente el ejercicio de los derechos que se consagran en este proyecto de ley. Asimismo, consideraron adecuado

que la Agencia de Protección de Datos vele por efectivo ejercicio de estos derechos.

Concluido el análisis de esta disposición, el señor Presidente de la Comisión la sometió a votación.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó el texto del proyecto del Ejecutivo, enmendado en los términos ya indicados.

Artículo 11

El artículo 11 de la ley N° 19.628 establece que el responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños.

Este precepto es reemplazado en el proyecto de ley del Ejecutivo por la siguiente disposición:

“Artículo 11.- Procedimiento ante el responsable de datos. Para ejercer los derechos que le reconoce esta ley, el titular debe presentar una solicitud o requerimiento escrito ante el responsable dirigido a la dirección de correo electrónico establecida para este fin o a través de un formulario de contacto o de un medio electrónico equivalente. La solicitud o el medio de contacto deben contener, a lo menos, las siguientes menciones:

a) Individualización del titular y de su representante legal o mandatario, según corresponda, y autenticación de su identidad de acuerdo a los procedimientos, formas y modalidades que establezca el reglamento.

b) Indicación de una dirección de correo electrónico o de otro medio electrónico equivalente para comunicar la respuesta.

c) Identificación de los datos personales o del tratamiento determinado, según corresponda, respecto de los cuales se ejerce el derecho correspondiente.

d) En las solicitudes de rectificación el titular debe indicar las modificaciones o actualizaciones precisas a realizar y acompañar, en su caso, los antecedentes que las sustenten. Cuando se trate de solicitudes de cancelación u oposición al tratamiento de datos, el titular debe indicar la causal o fundamento invocado para ello y acompañar también los

antecedentes que las sustenten, si correspondiere. En el caso del derecho de acceso, basta con la individualización del titular.

e) Cualquier otro antecedente que facilite la localización de los datos personales.

Recibida la solicitud, el responsable debe pronunciarse sobre ella inmediatamente o a más tardar dentro de los 10 días hábiles siguientes a la fecha de ingreso.

El responsable debe responder por escrito al titular a la dirección de correo electrónico fijada por éste. Cuando la respuesta se entregue por otro medio electrónico, el responsable debe almacenar los respaldos que le permitan demostrar la transmisión y recepción de la respuesta, su fecha y el contenido íntegro de ella.

En caso de denegación total o parcial de la solicitud, el responsable debe fundar su decisión indicando la causa invocada y los antecedentes que la justifican. En esta misma oportunidad, el responsable debe señalar al titular que dispone de un plazo de 10 días hábiles para formular una reclamación ante la Agencia de Protección de Datos Personales, de acuerdo al procedimiento establecido en el artículo 45.

Transcurridos los 10 días hábiles a que hace referencia el inciso segundo sin que haya respuesta del responsable, el titular puede formular directamente una reclamación ante la Agencia de Protección de Datos Personales, en los mismos términos del inciso anterior.

Cuando se formule una solicitud de rectificación o cancelación, el titular tiene derecho a solicitar y obtener del responsable el bloqueo temporal de los datos. La solicitud de bloqueo temporal debe ser fundada y el responsable deberá responder a este requerimiento dentro de los 2 días hábiles siguientes a su recepción. En caso de negativa, el responsable deberá invocar una causa justificada y fundar su respuesta.

La rectificación o cancelación de los datos se aplicarán sólo respecto de los responsables a quienes se les haya formulado la solicitud.”.

En relación a esta materia, la moción parlamentaria que se refunde en esta iniciativa regula, en su artículo 20, el denominado procedimiento de reclamación. El texto de esta proposición es el siguiente:

“Artículo 20. Procedimiento general. Si el responsable del registro o banco de datos no se pronunciare 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.”.

Al comenzar el estudio de esta materia, **los representantes del Ejecutivo, señora Piedrabuena y señor Godoy,** propusieron a la Comisión una nueva redacción para regular el procedimiento que se debe seguir ante el responsable de datos.

Esta disposición señala que para ejercer los derechos que le reconoce esta ley, el titular deberá presentar una solicitud o requerimiento escrito ante el responsable, dirigido a la dirección de correo electrónico establecida para este fin, a través de un formulario de contacto o un medio electrónico equivalente. La solicitud deberá contener, a lo menos, las siguientes menciones:

a) Individualización del titular y de su representante legal o mandatario, según corresponda y autenticación de su identidad de acuerdo a los procedimientos, formas y modalidades que establezca la Agencia de Protección de Datos Personales a través de una norma de carácter general dictada para este efecto;

b) Indicación de una dirección de correo electrónico o de otro medio electrónico equivalente para comunicar la respuesta;

c) Identificación de los datos personales o del tratamiento determinado, según corresponda, respecto de los cuales se ejerce el derecho correspondiente;

d) En las solicitudes de rectificación, el titular deberá indicar las modificaciones o actualizaciones precisas a realizar y acompañar, en su caso, los antecedentes que las sustenten. Cuando se trate de solicitudes de cancelación, el titular deberá indicar la causal invocada y acompañar los antecedentes que la sustenten, si correspondiere. Para las solicitudes de oposición, el titular deberá indicar la causal invocada y en el caso de la letra a) del artículo 8, deberá fundamentar brevemente su petición, podrá igualmente acompañar los antecedentes que estime procedentes. En el caso del derecho de acceso, bastará con la individualización del titular, y

e) Cualquier otro antecedente que facilite la localización de los datos personales.

Recibida la solicitud, el responsable deberá acusar recibo de ella y pronunciarse a más tardar dentro de los 15 días hábiles siguientes a la fecha de ingreso.

El responsable deberá responder por escrito al titular a la dirección de correo electrónico fijada por éste. Cuando la respuesta se entregue por otro medio electrónico, el responsable debe almacenar los respaldos que le permitan demostrar la transmisión y recepción de la respuesta, su fecha y el contenido íntegro de ella.

En caso de denegación total o parcial de la solicitud, el responsable deberá fundar su decisión indicando la causa invocada y los antecedentes que la justifican. En esta misma oportunidad, el responsable debe señalar al titular que dispone de un plazo de 15 días hábiles para formular una reclamación ante la Agencia de Protección de Datos Personales, de acuerdo al procedimiento establecido en el artículo 45.

Transcurrido el plazo de 15 días hábiles al que hace referencia el inciso segundo anterior, sin que haya respuesta del responsable, el titular podrá formular directamente una reclamación ante la Agencia de Protección de Datos Personales, en los mismos términos del inciso anterior.

Cuando se formule una solicitud de rectificación, cancelación u oposición, el titular tendrá derecho a solicitar y obtener del responsable, el bloqueo temporal de sus datos o del tratamiento que realice, según corresponda. La solicitud de bloqueo temporal deberá ser fundada y el responsable deberá responder al requerimiento dentro de los 2 días hábiles siguientes a su recepción. En tanto no resuelva esta solicitud, el responsable no podrá tratar los datos del titular que forman parte del requerimiento. En caso de rechazo, el responsable deberá fundar su respuesta y comunicar en forma electrónica su decisión a la Agencia de Protección de Datos Personales.

La rectificación, cancelación u oposición al tratamiento de los datos se aplicarán sólo respecto de los responsables a quienes se les haya formulado la solicitud.”.

Al iniciarse el estudio de esta materia, **el Presidente de la Comisión, Honorable Senador señor Harboe,** expresó que cuando en el inciso primero, se señala: “Para ejercer los derechos que le reconoce esta ley, el titular deberá presentar una solicitud o requerimiento escrito ante el responsable, dirigido a la dirección de correo electrónico establecida para este fin, a través de un formulario de contacto o un medio electrónico equivalente.”, es necesario también permitir la opción de que sea enviado a una dirección física, ya que si alguien no tiene acceso a correo electrónico no podrá ejercer estos derechos.

El asesor del Ministerio de Hacienda, señor Godoy, recalcó que el formulario de contacto se refiere a un documento físico.

En relación a la letra a), **el Honorable Senador, señor Larraín** sostuvo que debe revisarse su redacción, cuando dispone: “de acuerdo a los procedimientos, formas y modalidades que establezca la Agencia de Protección de Datos Personales a través de una norma de carácter general dictada para este efecto.”. Llamó la atención que la Agencia puede comenzar a dictar normas que agreguen otras materias y requisitos y asuma potestades que no le corresponden.

El asesor del Ministerio de Hacienda, señor Godoy precisó que la facultad que se le confiere, tiene que ver estrictamente con el tema de los medios de autenticación de la identidad del titular.

El Honorable Senador, señor Larraín propuso eliminar en la letra a), la siguiente frase: “a través de una norma de carácter general dictada para este efecto”.

Puesta en votación la letra a) del artículo 11 del nuevo texto propuesto por el Ejecutivo, fue aprobado con la enmienda señalada, por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Araya, Harboe y Larraín.

Luego, al analizar la letra b), **el Presidente de la Comisión, Honorable Senador señor Harboe** sugirió la siguiente redacción:

“b) Indicación de un domicilio o dirección de correo electrónico o de otro medio equivalente para comunicar la respuesta;”.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó esta disposición.

Respecto a la letra c) del texto propuesto por el Ejecutivo, **el Honorable Senador señor Larraín** propuso eliminar la expresión: “según corresponda,”.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó esta disposición con la enmienda indicada precedentemente.

A continuación, el Ejecutivo propuso un cambio en la letra d).

El asesor del Ministerio de Hacienda, señor Roberto Godoy propuso agregar la expresión: “no obstante”, a continuación de la siguiente oración: “Para las solicitudes de oposición, el titular deberá indicar la causal invocada y en el caso de la letra a) del artículo 8, deberá fundamentar brevemente su petición,”.

Dado lo anterior, la mencionada letra, quedaría de la siguiente manera:

“d) En las solicitudes de rectificación, el titular deberá indicar las modificaciones o actualizaciones precisas a realizar y acompañar, en su caso, los antecedentes que las sustenten. Cuando se trate de solicitudes de cancelación, el titular deberá indicar la causal invocada y acompañar los antecedentes que la sustenten, si correspondiere. Para las solicitudes de oposición, el titular deberá indicar la causal invocada y en el caso de la letra a) del artículo 8, deberá fundamentar brevemente su petición, **no obstante** podrá igualmente acompañar los antecedentes que estime procedentes. En el caso del derecho de acceso, bastará con la individualización del titular, y.”.

El Presidente de la Comisión, Honorable Senador señor Harboe puso en votación la sugerencia del Ejecutivo.

La Comisión, por la unanimidad de los Honorables Senadores presentes, señores Araya, De Urresti, Harboe y Larraín, la rechazaron.

En el estudio de los incisos posteriores, específicamente en el sexto, **el Honorable Senador señor Larraín** preguntó cómo sigue el procedimiento ante la solicitud de bloqueo temporal, luego que

el responsable funde su respuesta y comunique en forma electrónica su decisión a la Agencia de Protección de Datos Personales.

La asesora, señora Bernardita Piedrabuena sostuvo que el artículo 45 regula el procedimiento.

El asesor del Honorable Senador señor Larraín, señor Olmedo, destacó que se debe determinar si la actuación de la Agencia es de oficio o no. Preguntó qué efecto produce la comunicación a la Agencia.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena ratificó que es el titular quien tiene que reclamar ante la Agencia. Afirmó que esta última, en la situación planteada, no actuará de oficio.

El asesor del Honorable Senador Larraín, señor Olmedo, aseveró que el incumplimiento de parte del responsable ante una solicitud de bloqueo temporal, debe ser considerado como agravante en la aplicación de la multa.

El asesor del Ministerio de Hacienda, señor Godoy, aclaró que la Agencia debe actuar ante requerimiento del titular. Consignó que se está creando un incentivo para que el responsable sea cuidadoso en la ponderación de la solicitud de bloqueo.

El Presidente de la Comisión, Honorable Senador señor Harboe hizo presente que se debe buscar un mecanismo de sanción.

Asimismo, indicó que en el penúltimo inciso, también se debe hacer referencia al procedimiento consagrado en el artículo 45.

En relación a esta última inquietud, los representantes del Ejecutivo propusieron, mediante una indicación aprobar las demás disposiciones de este artículo, en los siguientes términos:

“e) Cualquier otro antecedente que facilite la localización de los datos personales. **(Unanimidad 3 x 0. Honorables Senadores señores Araya, Harboe y Larraín).**

Recibida la solicitud el responsable deberá acusar recibo de ella y pronunciarse a más tardar dentro de los 15 días hábiles siguientes a la fecha de ingreso.

El responsable deberá responder por escrito al titular a su domicilio o la dirección de correo electrónico fijada por éste. Cuando la respuesta se entregue por otro medio electrónico, el responsable debe almacenar los respaldos que le permitan demostrar la transmisión y recepción de la respuesta, su fecha y el contenido íntegro de ella.

En caso de denegación total o parcial de la solicitud, el responsable deberá fundar su decisión indicando la causa invocada y los antecedentes que la justifican. En esta misma oportunidad el responsable debe señalar al titular que dispone de un plazo de 15 días hábiles para formular una reclamación ante la Agencia de Protección de Datos Personales, de acuerdo al procedimiento establecido en el artículo 45.

Transcurrido el plazo de 15 días hábiles al que hace referencia el inciso segundo anterior, sin que haya respuesta del responsable, el titular podrá formular directamente una reclamación ante la Agencia de Protección de Datos Personales, en los mismos términos del inciso anterior.

Cuando se formule una solicitud de rectificación, cancelación u oposición, el titular tendrá derecho a solicitar y obtener del responsable el bloqueo temporal de sus datos o del tratamiento que realice, según corresponda. La solicitud de bloqueo temporal deberá ser fundada y el responsable deberá responder al requerimiento dentro de los dos días hábiles siguientes a su recepción. En tanto no resuelva esta solicitud, el responsable no podrá tratar los datos del titular que forman parte del requerimiento. En caso de rechazo el responsable deberá fundar su respuesta y comunicar en forma electrónica su decisión a la Agencia de Protección de Datos Personales. El titular podrá reclamar de esta decisión ante la Agencia de Protección de Datos Personales, aplicándose lo dispuesto en la letra i) del artículo 45.

La rectificación, cancelación u oposición al tratamiento de los datos se aplicarán sólo respecto de los responsables a quienes se les haya formulado la solicitud.”.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó el artículo 11, con las enmiendas ya reseñadas.

El texto acordado precedentemente fue ratificado mediante una indicación que presentó el Ejecutivo, la que se dio por aprobada con las votaciones señaladas precedentemente.

-.-.-

En una sesión posterior, la Comisión comenzó su trabajo analizando el artículo 21 contenido en la Moción parlamentaria, disposición que regula el interés colectivo en la protección de datos. Su texto es el siguiente:

“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.”.

El asesor del Ministerio de Hacienda, señor Godoy reconoció que el interés colectivo no es recogido en el Mensaje del Ejecutivo. Agregó que los datos personales, en esencia son de carácter personal. Por lo tanto, a diferencia de otros derechos fundamentales o de otros sistemas de protección jurídica, no se visualiza que existan intereses colectivos o difusos que requieran una tutela especial.

Atendida la explicación precedente, la Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores De Urresti, Harboe y Larraín, rechazó este precepto.

-.-.-

Artículo 12

Seguidamente, la Comisión consideró la propuesta para sustituir el artículo 12 de la ley N° 19.628, que da inicio a su título II y que establece los derechos de los titulares de datos.

Entre tales derechos se destacan, por ejemplo, la facultad de exigir a quien sea responsable de un banco de datos, información sobre antecedentes relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente.

Asimismo, a que se modifiquen los datos personales que sean erróneos, inexactos, equívocos o incompletos. Igualmente, a que se eliminen datos que su almacenamiento carezca de fundamento legal o cuando estuvieren caducos.

En relación a esta materia, el proyecto de ley del Ejecutivo propone sustituir íntegramente el Título II de la ley N° 19.628.

Para lograr ese objetivo propone, en primer lugar, incorporar a la ley un título II, nuevo, referido al tratamiento de los datos personales y de las categorías especiales de datos.

Asimismo, agrega un párrafo primero que regula el consentimiento del titular, de las obligaciones y deberes del responsable y del tratamiento de datos en general.

Teniendo en cuenta lo anterior, el proyecto de ley del Ejecutivo contiene un artículo 12 que dispone lo siguiente:

“Artículo 12.- Regla general del tratamiento de datos. Es lícito el tratamiento de los datos personales que le conciernen al titular, cuando otorgue su consentimiento para ello.

El consentimiento del titular debe ser libre, informado y específico en cuanto a su finalidad o finalidades. El consentimiento debe manifestarse de manera inequívoca, mediante una declaración verbal, escrita o expresada a través de un medio electrónico equivalente, o mediante un acto afirmativo que dé cuenta con claridad de la voluntad del titular.

Cuando el consentimiento lo otorgue un mandatario, deberá encontrase expresamente premunido de esta facultad.

El titular puede revocar el consentimiento otorgado en cualquier momento y sin expresión de causa, utilizando medios similares o equivalentes a los empleados para su otorgamiento. La revocación del consentimiento no tendrá efectos retroactivos.

Los medios utilizados para el otorgamiento o la revocación del consentimiento deben ser expeditos, fidedignos, gratuitos y estar permanentemente disponibles para el titular.

El consentimiento no se considerará una base jurídica suficiente para la validez del tratamiento de datos, cuando exista un desequilibrio ostensible entre la posición del titular y el responsable.

Corresponde al responsable probar que el tratamiento de datos realizado contó con el consentimiento del titular.”.

Al comenzar el estudio de esta proposición de enmienda, la Comisión tuvo presente que la moción parlamentaria que se

refunde con este proyecto considera un artículo 5° que regula también la figura del consentimiento del titular de datos. Su texto es el siguiente:

"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.".

Luego de tomar nota de estos antecedentes, el señor Presidente de la Comisión concedió el uso de la palabra al **asesor del Ministerio de Hacienda, señor Godoy,** quien manifestó que estamos ante una de las normas centrales del proyecto de ley en estudio, dado que recoge principio fundante para el tratamiento de datos, cual es el consentimiento del titular.

Seguidamente, propuso aprobar el proyecto de ley presentado por el Ejecutivo, sustituyendo sus dos incisos finales por los siguientes:

“El consentimiento no se considerará una base jurídica suficiente para la validez del tratamiento de datos, cuando exista un desequilibrio ostensible entre la posición del titular y el responsable.

Corresponde al responsable probar que el tratamiento de datos realizado contó con el consentimiento del titular”.

Expresó que el artículo del proyecto de ley del Ejecutivo regula explícitamente las bases del consentimiento, en armonía con su definición. Precisó que la regla general, para estos efectos, es que el consentimiento debe expresarse de manera inequívoca.

El Honorable Senador señor Larraín solicitó una explicación respecto al penúltimo inciso del artículo 12 del texto refundido, que dispone: “El consentimiento no se considerará una base jurídica suficiente para la validez del tratamiento de datos, cuando exista un desequilibrio ostensible entre la posición del titular y el responsable.”.

El asesor del Ministerio de Hacienda, señor Godoy aseveró que la norma estaba incorporada en la Moción, y se refiere a la ratificación de la expresión de un consentimiento libre. Es decir, exento de vicios.

El Presidente de la Comisión, Honorable Senador señor Harboe sostuvo que aquí surge la discusión respecto a los contratos de adhesión. Declaró que en ellos no existe consideración respecto de la voluntad de una de las partes. Lo anterior otorga celeridad a la celebración del acto jurídico.

Remarcó que, muchas veces, para suscribir un contrato, por ejemplo, de cuenta corriente, el banco exige a la otra parte que confiera permiso para el tratamiento de datos. Ello se puede entender, siempre y cuando, el tratamiento persiga la finalidad del contrato principal.

Constató que el inciso antes referido, busca evitar que el consentimiento del titular sea obligado.

El asesor del Comité Udi, señor Mery, destacó que el hecho de que exista un “desequilibrio ostensible”, no nos lleva forzosamente a la conclusión de que falte el consentimiento o que éste tuviese un vicio.

El Presidente de la Comisión, Honorable Senador señor Harboe aseveró que el texto dice que el consentimiento no se considerará una base jurídica suficiente para la validez del tratamiento de datos, cuando exista un desequilibrio ostensible entre la posición del titular y el responsable. Lo anterior implica que el mencionado desequilibrio puede considerarse como base, pero se exigen más elementos.

El asesor del Honorable Senador señor Larraín, señor Mery, subrayó que la introducción de dicho concepto puede producir problemas a futuro. Recalcó que éste no existe como criterio general dentro del derecho de los contratos. Las leyes, argumentó, no han definido este asunto.

El asesor del Comité PPD, señor Sebastián Abarca, precisó que el inciso en discusión debe ser estudiado conjuntamente con el inciso final, porque en este último, se establece el *onus probandi.* Connotó que al tratador de los datos le corresponderá probar que el titular otorgó su consentimiento. De manera que el desequilibrio ostensible, *per se*, no trae aparejado una sanción.

Sometido a votación el artículo 12 fue aprobado por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores De Urresti, Harboe y Larraín.

En una sesión posterior**, el abogado asesor del Ministerio de Hacienda, señor Godoy**, propuso a la Comisión reabrir el debate del artículo 12, con el fin de introducir dos enmiendas a su articulado.

La primera, consiste en agregar, en el inciso tercero, luego de la coma, la palabra “éste”.”.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, De Urresti, Harboe y Larraín, aprobó esta enmienda del Ejecutivo.

La segunda, implica reemplazar el inciso sexto por el siguiente:

“Al evaluar si el consentimiento se ha prestado libremente, se tendrá en consideración el hecho que haya sido otorgado para la ejecución de un contrato o la prestación de un servicio que no requiere del tratamiento de datos para su ejecución o cumplimiento. En tales circunstancias, el consentimiento no se considerará una base jurídica suficiente para la validez del tratamiento de datos.”.”

El Presidente de la Comisión, Honorable Senador señor Harboe, precisó que en el texto original se establece que el

consentimiento, que es una de las fuentes de licitud en el tratamiento de datos, no tendrá valor cuando haya un desequilibrio ostensible entre el titular del dato y quien efectúe el tratamiento.

Agregó que el cambio propuesto por el Ejecutivo consiste en evaluar si el consentimiento se ha prestado libremente, y no se considera la diferencia de posición entre el titular y el tratador de datos.

Señaló que puede ocurrir, por ejemplo, que una empresa con la que se contrata un crédito de consumo exige ciertos datos para fines relacionados con dicho crédito. Aseveró que si posteriormente esa empresa utiliza la información para fines distintos, se puede considerar que el consentimiento del titular se está extendiendo a una actividad disímil.

Recalcó que la redacción sugerida no es precisa. Acotó que la situación se podría solucionar si existe la posibilidad de invocar una norma distinta, en que apelando al principio de finalidad se evite que los datos sean utilizados para un fin distinto para el cual se prestó el consentimiento.

El Honorable Senador señor De Urresti connotó que no se define adecuadamente lo que es el desequilibrio ostensible. Hizo presente que la norma propuesta solo hace referencia a la circunstancia de haberse prestado libremente el consentimiento.

Añadió que la definición jurídica del desequilibrio ostensible constituye un elemento fundamental. Remarcó que éste debiera precisarse con mayor rigurosidad.

El asesor del Ministerio de Hacienda, señor Godoy expresó que es posible realizar tratamiento con otras finalidades, sin solicitar el consentimiento, en la medida que los fines sean compatibles.

Indicó que la disposición sobre la diferencia ostensible, proviene de la moción. Ella señala en su artículo 5°, inciso segundo, lo siguiente:

“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.”.

Agregó que se ha tratado de vincular la diferencia ostensible a los contratos de adhesión y a aquellos casos en que no se requería el consentimiento del titular para que traten sus datos.

Asimismo, indicó que el término “diferencia ostensible” es una cuestión compleja de definir. Expuso que ello debiese quedar a la decisión de los tribunales.

El Presidente de la Comisión, Honorable Senador señor Harboe, destacó que la moción contempla dos hipótesis. La primera, se refiere al caso en que el otorgamiento del consentimiento se considera como condición para poder celebrar un contrato. La segunda dice relación que cuando existe un desequilibrio claro entre la posición del titular y el responsable, el consentimiento carecerá de validez. Subrayó que esta última hipótesis no fue considerada en la propuesta del Ejecutivo.

El Honorable Senador señor De Urresti hizo presente que es relevante establecer ciertos parámetros en relación al desequilibrio ostensible.

El Honorable Senador señor Larraín consideró confusa y compleja la forma en que se resuelve este tema en la propuesta que ha presentado el Ejecutivo.

El Presidente de la Comisión, Honorable Senador señor Harboe connotó que el nuevo inciso sexto propuesto por el Ejecutivo elimina el desequilibrio ostensible del proyecto. Sugirió mantener la redacción ya aprobada por la Comisión.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, De Urresti, Harboe y Larraín, rechazó la nueva propuesta de redacción del inciso sexto de este artículo.

Artículo 13

A continuación, la Comisión consideró la sustitución del artículo 13 de la ley N° 19.628, disposición que establece 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.

En su reemplazo el proyecto de ley del Ejecutivo consigna un artículo 13, nuevo, que regula diversas situaciones en que no se requiere el consentimiento del titular de datos para tratar los antecedentes que se indican. Su texto es el siguiente:

“Artículo 13.- Excepciones al consentimiento. No se requiere el consentimiento del titular en los siguientes casos:

a) Cuando el tratamiento se refiere a datos personales que han sido recolectados de una fuente de acceso público.

b) Cuando el tratamiento esté referido a datos relativos a obligaciones de carácter económico, financiero, bancario o comercial y se realice de conformidad con las normas del título III de esta ley.

c) Cuando el tratamiento sea necesario para la ejecución o el cumplimiento de una obligación legal o de un contrato en que es parte el titular.”.

Al iniciarse el estudio de esta disposición, los representantes del Ejecutivo sugirieron a la Comisión aprobar este artículo con algunos cambios. La norma propuesta es la siguiente.

“Artículo 13.- Otras fuentes de licitud del tratamiento de datos. Es lícito el tratamiento de datos personales, sin el consentimiento del titular, en los siguientes casos:

a) Cuando los datos han sido recolectados de una fuente de acceso público y su tratamiento esté relacionado con los fines para los cuales fueron entregados o recogidos.

b) Cuando el tratamiento esté referido a datos relativos a obligaciones de carácter económico, financiero, bancario o comercial y se realice de conformidad con las normas del Título III de esta ley.

c) Cuando el tratamiento sea necesario para el cumplimiento de una obligación legal.

d) Cuando el tratamiento de datos sea necesario para la ejecución de un contrato en que es parte el titular.

e) Cuando el tratamiento sea necesario para la satisfacción de intereses legítimos del responsable o de un tercero, siempre que con ello no se afecten los derechos y libertades fundamentales del titular.

f) Cuando el tratamiento de datos lo disponga la ley.

El responsable deberá acreditar la licitud del tratamiento de datos.”.

La Comisión analizó, en primer lugar, la letra a) de esta nueva redacción.

El asesor del Honorable Senador señor Larraín, señor Olmedo, indicó que era razonable aprobar esta letra. Agregó que los problemas que se pueden presentar en esta materia serán resueltos por la Agencia de Protección de Datos, organismo que tendrá, como se explicará más adelante, la facultad de resolver las dudas o controversias que se susciten sobre si una determinada base de datos es considerada fuente de acceso público e identificar categorías genéricas, clases o tipos de datos, conjuntos de datos o bases de datos que posean esta condición.

Seguidamente, **el señor Presidente de la Comisión** sometió a votación la letra a) del artículo 13, contenida en la redacción alternativa sugerida por el Ejecutivo.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores De Urresti, Harboe y Larraín, aprobó, sin enmiendas, esta disposición.

A continuación, el señor Presidente de la Comisión puso en discusión la letra b) del artículo 13.

En relación a esta letra, **la asesora del Ministerio de Economía, señora Bernardita Piedrabuena,** afirmó que el Título III se regula la información y el uso de la información de datos económicos. Recordó que la ley N° 20.575 permite utilizarlos para verificar la capacidad crediticia del deudor.

Asimismo, indicó que en la legislación comparada se ha señalado que en el caso de los datos económicos no se exige el consentimiento, dado que hay terceros involucrados y es de interés público conocer esos antecedentes. Precisó que esto es fundamental para el normal funcionamiento del mercado crediticio.

Concluyó que, sin perjuicio de lo anterior el titular de los datos es siempre dueño de ellos.

El Presidente de la Comisión, Honorable Senador señor Harboe, enfatizó que es importante determinar qué normas que regulen los datos económicos y comerciales se pueden incorporar en el presente proyecto, específicamente en el Título III.

Sugirió agregar en la presente iniciativa lo dispuesto en la ley N° 20.575, normativa que establece el principio de finalidad en el tratamiento de datos personales.

Concluido el análisis de esta disposición, el Presidente, señor Harboe, la sometió a votación.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores De Urresti, Harboe y Larraín, aprobó la letra b) del artículo 13.

En seguida, el señor Presidente de la Comisión puso en discusión la letra c).

La asesora del Ministerio de Economía, señora Piedrabuena, hizo presente que había cierta similitud entre lo que prescribe la letra en discusión y la letra f), del mismo artículo.

Se recordó que la letra c) establece lo siguiente:

“c) Cuando el tratamiento sea necesario para el cumplimiento de una obligación legal.”.

Por su parte la letra f) prescribe: “f) Cuando el tratamiento de datos lo disponga la ley.”.

El asesor del Comité Udi, señor Mery manifestó que pese a la semejanza entre ambas letras, éstas no son idénticas. Aclaró que cuando se habla de una obligación legal, se refiere a obligaciones que no tienen una fuente contractual. Puso como ejemplo las pensiones alimenticias adeudadas y el cumplimiento de obligaciones tributarias.

El asesor del Ministerio de Hacienda, señor Godoy, sugirió a la Comisión refundir ambas letras en la siguiente redacción: “c) Cuando el tratamiento sea necesario para el cumplimiento de una obligación legal o lo disponga la ley.”.

Puesta en votación la letra c), con la enmienda señalada, fue aprobada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores De Urresti, Harboe y Larraín.

En una sesión posterior, los representantes del Ejecutivo sugirieron agregar, en la letra c) antes de la palabra “cumplimiento” las expresiones “la ejecución o”.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, De Urresti, Harboe y Larraín, aprobó esta enmienda.

A continuación, se analizó la **letra d) del artículo 13**. En relación a este precepto, el asesor del Ministerio de Hacienda, señor Godoy, propuso una nueva redacción:

"d) Cuando el tratamiento de datos sea necesario para la celebración o ejecución de un contrato entre el titular y el responsable, o para la ejecución de medidas precontractuales adoptadas a solicitud del titular."

El Presidente de la Comisión, Honorable Senador, señor Harboe expresó que en la práctica, sobre todo en materia de contratos a distancia, se genera necesidad de intercambio de datos. Preguntó cómo se protegen los datos del titular si éste los entrega en la etapa precontractual, y no llega a celebrarse el contrato.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena aseveró que al no perfeccionarse el contrato, los datos carecen de fuente de legitimidad. Por lo tanto, éstos deben anonimizarse.

El Presidente de la Comisión, Honorable Senador señor Harboe se mostró partidario de aprobar la propuesta del Ejecutivo, pero que se consigne la obligación de establecer en una norma posterior, que tratándose de datos entregados en una relación precontractual, en el evento de no concretarse, éstos tendrán que ser eliminados o anonimizados.

El Honorable Senador señor Larraín precisó que los datos que se entregan para la etapa preparatoria de un contrato, se pueden utilizar, al menos que no se perfeccione, en cuyo caso se deberán anonimizar.

El Presidente de la Comisión, Honorable Senador señor Harboe, advirtió que es importante dejar consignado que si la relación precontractual no llega a materializarse en un contrato, el titular podrá pedir el retiro o la anonimización de los datos.

La Comisión, por la unanimidad de sus miembros presentes, los Honorables Senadores señores Araya, De Urresti, Harboe y Larraín, aprobó la letra d).

A continuación, la Comisión consideró la **letra e)** del artículo 13. Su texto es el siguiente:

“e) Cuando el tratamiento sea necesario para la satisfacción de intereses legítimos del responsable o de un tercero, siempre que con ello no se afecten los derechos y libertades fundamentales del titular.”.

En relación a este precepto, **la asesora del Ministerio de Economía, señora Piedrabuena,** aseveró que es el responsable quien tiene el deber de probar que está cumpliendo con un interés legítimo, que no afecta los derechos fundamentales del titular y que, si fuera el caso, en esa ponderación, puede aplicar mitigadores y éstos pueden llegar a permitir que se utilicen los datos.

Afirmó que es una fuente que exige una mayor fundamentación por parte del responsable.

El asesor del Honorable Senador señor Larraín, señor Olmedo, sostuvo que la manera de proteger a los titulares está dada por el artículo 14 ter. En la letra d), del mencionado artículo, se impone el deber de publicidad de estas materias en las páginas web de los responsables. Llamó la atención que dicho artículo hace referencia a los responsables, y la letra e), en estudio, hace mención al responsable o un tercero. Manifestó que le surge la inquietud sobre si la obligación de transparencia también se aplica respecto al tercero, o se reduce solo al responsable.

El asesor del Ministerio de Hacienda, señor Godoy, indicó que la obligación de transparencia que consagra el artículo 14 ter, recae sobre el responsable.

El Presidente de la Comisión, Honorable Senador señor Harboe manifestó tener una duda en esta materia, porque se plantea como excepción al consentimiento, la satisfacción de intereses legítimos del responsable. Ejemplificó con el caso de una empresa que determina que posee el legítimo interés de tener una base de datos de todos los asesores de los parlamentarios.

Llamó la atención que la expresión “fundamentales” que utiliza esta letra, se puede interpretar como derechos constitucionales, cuando lo que se pretende es resguardar los derechos de acceso, cancelación, rectificación y de oposición.

Dado lo anterior, sugirió eliminar el término antes mencionado, ya que más que elevar la categoría, lo puede terminar restringiendo.

El asesor del Ministerio de Hacienda, señor Godoy, precisó que respecto a la expresión “intereses legítimos”, en el texto refundido se configuran dos situaciones que se consideran como tal. Una de ellas dice relación con el tratamiento de datos que hacen las instituciones sin fines de lucro, respecto de sus asociados. El otro corresponde a todos aquellos tratamientos que se hacen con fines históricos, científicos o estadísticos. Constató que el mencionado interés, dice relación con un cierto valor público-social, no necesariamente colectivo. Detalló que cualquier responsable no puede atribuirse un interés en beneficio propio para efecto de constituir una base de datos e invocar un interés legítimo.

Puesta en votación la letra e), con la supresión de la expresión “fundamentales”, fue aprobada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores De Urresti, Harboe y Larraín.

En seguida, **los representantes del Ejecutivo** sugirieron a la Comisión incorporar la siguiente letra f), nueva:

“f) Cuando el tratamiento de datos sea necesario para la formulación, ejercicio o defensa de un derecho ante los tribunales de justicia.”.

El asesor del Ministerio de Hacienda, señor Godoy sostuvo que se establece una causal de legitimidad del tratamiento cuando éste sea indispensable para la formulación, ejercicio o defensa de un derecho. Connotó que en ciertas ocasiones no será posible recurrir al consentimiento para efectos de poder habilitar el ejercicio de una acción ante los tribunales de justicia.

El asesor del Honorable Senador Larraín, señor Olmedo estimó que la norma propuesta por el Ejecutivo es muy amplia y vaga. Estimó que ella debe ser acotada a las materias que trata esta iniciativa, es decir, a las controversias que surjan entre la Agencia y los responsables de datos. Agregó que ampliarlo a cualquier procedimiento en sede jurisdiccional lo considera un exceso.

El Presidente de la Comisión, Honorable Senador señor Harboe, consultó por el efecto práctico de aprobar una disposición como la que se propone.

El asesor del Honorable Senador Larraín, señor Olmedo destacó que ella podría producir efecto en la configuración de bases de datos en sede civil que lleguen a generar algún tipo de información que no se encuentre sistematizada.

El Presidente de la Comisión, Honorable Senador señor Harboe, constató que en la actualidad existen bases de datos conformadas a partir de la información que se obtiene de los propios tribunales. Inquirió si la norma sugerida busca legitimar el tratamiento de datos antes mencionado.

El asesor del Ministerio de Hacienda, señor Godoy manifestó que la disposición busca que una persona pueda accionar en contra de otra, recurriendo a información personal sin necesidad de requerir del consentimiento de esta última. Todo ello con la finalidad de defender un derecho o ejercer una acción ante los tribunales de justicia.

Añadió que es indispensable que el conflicto debe estar ventilándose en sede jurisdiccional.

El Presidente de la Comisión, Honorable Senador señor Harboe consideró adecuado no exigir el consentimiento de un potencial demandado para poder insertar sus datos en una demanda. Sin embargo, el tratamiento de datos es más amplio que solo usar los datos. Por lo tanto, no es partidario de utilizar aquella expresión.

Aseveró que el tratamiento de datos ha sido definido en este cuerpo legal como cualquier operación o conjunto de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, procesar, almacenar, comunicar, transmitir o utilizar de cualquier forma datos personales o conjuntos de datos personales.

El Honorable Senador señor Larraín constató que estamos en presencia de una hipótesis que parece razonable, en la cual el eventual afectado tiene cómo defenderse. Agregó que al ejercerse el derecho en un tribunal, este último puede oponerse.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena sostuvo que la norma sugerida por el Ejecutivo le otorga legitimidad al tratamiento de datos. Agregó que los datos sólo se tratan para la finalidad indicada.

Confirmó que independiente de cual sea la fuente de legitimidad, los derechos de los titulares están siempre resguardados.

El Presidente de la Comisión, Honorable Senador señor Harboe declaró cerrado el debate y sometió a votación la nueva letra f) presentada por el Ejecutivo.

La Comisión, por mayoría de votos de sus miembros presentes, aprobó la letra f) propuesta por el Ejecutivo. Se

pronunciaron a favor los Honorables Senadores señores Araya y Larraín. Se abstuvo el Honorable Senador señor Harboe.

A continuación, la Comisión consideró el inciso final del artículo 13, disposición que prescribe que el responsable deberá acreditar la licitud del tratamiento de datos.

Al iniciarse el estudio de este asunto, **el asesor del Comité Udi, señor Héctor Mery** connotó que la regla antes mencionada altera el orden natural de la carga de la prueba. Además, si se compara la situación de cada una de las letras precedentes, pareciera que el inciso en estudio puede ser válido respecto de solo algunas.

El asesor del Comité PPD, señor Sebastián Abarca aseveró que en materia probatoria también se admite cierto dinamismo. Destacó que la tendencia moderna consiste en que debe probar quien posee los medios para hacerlo. Añadió que el responsable del tratamiento siempre tratará de acreditar que su conducta es lícita. Afirmó que el inciso en estudio debería aprobarse.

El Honorable Senador señor Larraín hizo presente que se justifica la regla, porque constituye una excepción.

El Presidente de la Comisión, Honorable Senador señor Harboe expresó que la ley debe hacerse cargo de realidades económicas, sociales y también tecnológicas. Precisó que hoy resultaría prácticamente imposible para el titular de un dato poder probar la ilicitud del tratamiento cuando desconoce quién lo está desarrollando, y cuál fue su fuente de origen.

Dado lo anterior, consideró necesario aprobar esta disposición.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores De Urresti, Harboe y Larraín, aprobó este inciso.

Artículo 14

A continuación, la Comisión trató la enmienda al artículo 14 de la ley N° 19.628, disposición que señala que 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.

Respecto de esta disposición, el Mensaje del Ejecutivo propone su sustitución por la siguiente disposición:

“Artículo 14.- Obligaciones del responsable de datos. El responsable de datos, sin perjuicio de las demás disposiciones previstas en esta ley, tiene las siguientes obligaciones:

a) Informar y poner a disposición del titular, de manera expedita y cuando le sean requeridos, los antecedentes que acrediten la licitud del tratamiento de datos que realiza.

b) Asegurar que los datos personales se recojan con fines específicos, explícitos y lícitos, y que su tratamiento se limite al cumplimiento de estos fines.

c) Comunicar o ceder, en conformidad a las disposiciones de esta ley, información exacta, completa y veraz.

d) Cumplir con los demás principios que rigen el tratamiento de los datos personales previstos en esta ley.”.

En relación a esta materia, la moción parlamentaria que se refunde con esta iniciativa propone regular las obligaciones del responsable de datos, en los siguientes términos:

“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.”.

Al iniciarse el estudio de ambas proposiciones, el grupo de asesores parlamentarios sugirió a la Comisión acoger la norma contenida en el proyecto de ley del Ejecutivo.

En consecuencia, **el señor Presidente de la Comisión** puso en discusión el encabezado del artículo 14 y su letra a). Su texto es el siguiente:

“Artículo 14.- Obligaciones del responsable de datos. El responsable de datos, sin perjuicio de las demás disposiciones previstas en esta ley, tiene las siguientes obligaciones:

a) Informar y poner a disposición del titular, de manera expedita y cuando le sean requeridos, los antecedentes que acrediten la licitud del tratamiento de datos que realiza;”.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores De Urresti, Harboe y Larraín, aprobó estas disposiciones.

En seguida, el señor Presidente de la Comisión puso en discusión la letra b). Su texto es el siguiente:

“b) Asegurar que los datos personales se recojan con fines específicos, explícitos y lícitos, y que su tratamiento se limite al cumplimiento de estos fines;”.

En relación a esta letra, **el Presidente de la Comisión, Honorable Senador señor Harboe**, sugirió agregar la expresión: “de fuentes de acceso lícitas”, a continuación del término “recojan”. Afirmó

que si ello no es incorporado, se da pie para que las empresas adquieran bases de datos ilegales.

Puesta en votación la letra b), con la enmienda señalada, fue aprobada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores De Urresti, Harboe y Larraín.

A continuación, **el señor Presidente de la Comisión** puso en discusión lo prescrito en la letra c) del artículo 14. Su texto es el siguiente:

"c) Comunicar o ceder, en conformidad a las disposiciones de esta ley, información exacta, completa y veraz, y".

Respecto a esta letra c), **el asesor del Comité Udi, señor Mery**, consultó si el término información se utiliza en el sentido amplio de la palabra.

El Presidente de la Comisión, Honorable Senador señor Harboe, aclaró que la mencionada letra no dice relación con la libertad de opinión ni de información.

El asesor del Honorable Senador señor Larraín, señor Olmedo, se mostró partidario de clarificar el vocablo veraz.

El Presidente de la Comisión, Honorable Senador señor Harboe, recordó que la veracidad dice relación con el principio de calidad. Agregó que ella busca que el dato que se almacenará permita una identificación real y no distorsionada de las personas.

El asesor del Ministerio de Hacienda, señor Godoy, señaló que al estudiar el principio de calidad se llevó a cabo la mencionada discusión. Expresó que las calificaciones que se emplearon fueron datos: exactos; completos y actuales. Propuso utilizar la misma nomenclatura, reemplazando veraz por actual.

Puesta en votación la letra c) del texto refundido, con la enmienda de reemplazar la expresión "veraz" por "actual", fue aprobada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores De Urresti, Harboe y Larraín.

Seguidamente, los representantes del Ejecutivo propusieron incorporar en este artículo la siguiente letra d), nueva:

“d) Cancelar o anonimizar los datos personales del titular cuando fueron obtenidos para la ejecución de medidas precontractuales.”.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó la enmienda del Ejecutivo.

Seguidamente, la Comisión examinó la letra d) del proyecto de ley del Ejecutivo, que ha pasado a ser letra e). Su texto es el siguiente:

“e) Cumplir con los demás principios que rigen el tratamiento de los datos personales previstos en esta ley.

Puesta en votación esta nueva letra e) fue aprobada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores De Urresti, Harboe y Larraín.

Artículo 14 bis

Seguidamente, la Comisión consideró la posibilidad de incorporar una norma que regule el deber de secreto o confidencialidad.

En relación con esta materia, el proyecto de ley del Ejecutivo propone agregar a la ley N° 19.628 un artículo 14 bis, nuevo. Su texto es el siguiente:

“Artículo 14 bis.- Deber de secreto o confidencialidad. El responsable de datos está obligado a mantener secreto o confidencialidad acerca de los datos personales que conciernan a un titular, salvo aquellos que provengan de fuentes de acceso público o el titular los ha hecho manifiestamente públicos. Este deber subsiste aún después de concluida la relación con el titular.

El deber de secreto o confidencialidad no obsta a las comunicaciones o cesiones de datos que deba realizar el responsable en conformidad a la ley, y al cumplimiento de la obligación de dar acceso al titular e informar el origen de los datos, cuando esta información le sea requerida por el titular o por un órgano público dentro del ámbito de sus competencias legales.

El responsable debe adoptar las medidas necesarias con el objeto que sus dependientes o las personas naturales o jurídicas que ejecuten operaciones de tratamiento de datos bajo su

responsabilidad, cumplan el deber de secreto o confidencialidad establecidos en este artículo.

Quedan sujetas a la obligación de secreto o confidencialidad las personas e instituciones y sus dependientes que, en cumplimiento de una obligación legal, han remitido información a un organismo público sujeto al régimen de excepciones establecido en el artículo 24, en cuanto al requerimiento y al hecho de haber remitido dicha información.”.

Al analizar esta materia, la Comisión también tuvo a la vista el artículo 27 contenido en la Moción que se refunde en este informe con el proyecto de ley del Ejecutivo. Su texto es el siguiente:

“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.”.

Al comenzar el estudio de estos preceptos, los representantes del Ejecutivo sugirieron a la Comisión aprobar el artículo 14 bis.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena, destacó que el artículo está en línea con los principios de responsabilidad y confidencialidad. En él se establece que cuando un organismo público le solicite datos a un privado, en virtud de una obligación legal, ellos deben guardar secreto del envío. Ejemplificó con la información solicitada por la Unidad de Análisis Financiero a una institución bancaria. Esta última no puede informar del requerimiento al eventual sospechoso.

El Presidente de la Comisión, Honorable Senador señor Harboe, hizo presente que la responsabilidad se circunscribe al responsable y se excluye al encargado. Preguntó qué sucede con la situación de los empleados que entregan información.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena, ratificó que la ley clarifica que es el responsable el que debe velar por el cumplimiento de los principios y por los derechos de los titulares. Agregó que el responsable deberá repetir, si corresponde, sobre las personas que trabajen manejando los datos. Detalló que, en el sector privado, la persona que incumpla con los estándares de protección de datos sufrirá las consecuencias que se establezca en su contrato de trabajo. Respecto al sector público, indicó que las personas están llamadas a respetar el deber de secreto y reserva.

El Presidente de la Comisión, Honorable Senador señor Harboe, sostuvo que es necesario tener una discusión sobre este tema y buscar una disposición que corrija ciertas prácticas que se producen actualmente. Añadió que el deber de secreto no solo asiste al responsable, sino que también al personal que trabaja en la institución respectiva.

Indicó que la violación del secreto constituye un tipo penal. Reconoció que se puede perseguir la responsabilidad penal de violación de secreto, en el evento de que se extienda esta prohibición, no solo al responsable, sino a quienes trabajan con él.

Agregó que la lógica que opera en el mundo privado, de someter al trabajador solo a la sanción que establezca el contrato, podría llegar a constituir una exención de responsabilidad bien delicada. Presentó las siguientes hipótesis: Un primer caso puede consistir en que la Agencia de Protección de Datos sanciona a una institución por vulneración del principio del secreto y el empleador no ejecuta ninguna acción respecto al trabajador. Se produce una impunidad total respecto al dependiente. En un segundo caso, el empleador decide despedir al trabajador y éste acude a otra empresa en su calidad de experto en protección de datos. Se preguntó ¿queremos que esa persona deambule por el mercado, a pesar de haber infringido manifiestamente su obligación de reserva?

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena, manifestó que todas las personas tienen el derecho al olvido. Respecto a la contratación del trabajador despedido por vulnerar el secreto, cifró sus esperanzas en el mercado laboral y específicamente a las referencias laborales que éste deba presentar.

El Honorable Senador señor Larraín indicó que se podría agregar que las obligaciones que le corresponden al responsable se extenderán a quienes trabajen con él. Enfatizó que lo anterior no necesariamente cierra el círculo, porque si se quiere filtrar la información, ésta se puede entregar a terceros, para que ellos infrinjan el deber antes mencionado.

El asesor del Honorable Senador señor Larraín, señor Olmedo expresó que los términos secreto; reserva y confidencialidad son distintos. Precisó que el vocablo “secreto”, lo entiende dentro del secreto estatal. Subrayó que en el ámbito en que se aplicará la presente iniciativa, estimó más adecuado utilizar la palabra “reserva”.

Estimó que se debe contemplar un mecanismo legal para proteger al funcionario que se percata que el responsable está incurriendo en una infracción grave y opta por denunciarlo.

El asesor del Ministerio de Hacienda, señor Godoy, aseveró que la regla que se consagra en el artículo, está establecida en beneficio del titular. Remarcó que se objetiviza la responsabilidad.

Respecto a la diferencia de secreto y confidencialidad, ésta radica en el origen. El secreto surge de la ley y la confidencialidad del acuerdo entre las partes.

El Presidente de la Comisión, Honorable Senador señor Harboe afirmó que despejado los conceptos de secreto y confidencialidad y aclarado que la norma busca proteger al titular, está en condiciones de aprobar el artículo 14 bis.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores De Urresti, Harboe y Larraín, aprobó este artículo del proyecto de ley del Ejecutivo, sin enmiendas.

Artículo 14 ter

En una sesión posterior, la Comisión analizó la proposición del Gobierno de incorporar un artículo 14 ter a la ley N° 19.628. Su texto es el siguiente:

“Artículo 14 ter.- Deber de información y transparencia. El responsable de datos debe mantener permanentemente a disposición del público, en su sitio web o en cualquier otro medio de información equivalente, al menos, la siguiente información:

a) La política de tratamiento de datos personales que ha adoptado, la fecha y versión de la misma.

b) La individualización del responsable de datos, su representante legal, y la identificación del encargado de prevención si existiere.

c) La dirección de correo electrónico, el formulario de contacto o la identificación del medio tecnológico equivalente a través del cual se le notifican las solicitudes que realicen los titulares.

d) Las categorías, clases o tipos de bases de datos que administra; la descripción genérica del universo de personas que comprenden las bases de datos; los destinatarios a los que se prevé comunicar o ceder los datos; y las finalidades del tratamiento que realiza.

e) La política y las medidas de seguridad adoptadas para proteger las bases de datos personales que administra.”.

Igualmente, al considerar esta disposición la Comisión tuvo a la vista los artículos 28 y 29 de la moción parlamentaria que se refunde en este informe. Su texto es el siguiente:

“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 regirá 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 estipulara, 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;

e) 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.”.

Al iniciarse el análisis de estos preceptos, el Ejecutivo presentó una indicación que mantiene el artículo 14 ter propuesto por el Gobierno, con la enmienda de agregar las siguientes letras f) y g), nuevas:

“f) El derecho que le asiste al titular para solicitar ante el responsable, acceso, rectificación, cancelación, oposición y portabilidad de sus datos personales, de conformidad a esta ley, y

g) El derecho que le asiste al titular de recurrir ante la Agencia de Protección de Datos Personales, en caso que el responsable rechace o no responda oportunamente las solicitudes que le formule.”.

El asesor del Ministerio de Hacienda, señor Godoy, señaló que la propuesta del Ejecutivo fue complementada con un par de ideas contenidas en la Moción parlamentaria. Agregó que en un solo artículo se consagran las obligaciones de transparencia e información que recaen sobre los responsables de datos.

El Presidente de la Comisión, Honorable Senador señor Harboe, precisó que en la moción se habla de responsable y del encargado, y en el texto refundido solo se menciona al responsable. Añadió que en el proyecto de ley presentado por los Honorables Senadores, se establecía la obligación de tener un registro de las actividades del tratamiento. Es decir, no solo de la política que adhieren, sino que también de las acciones que están realizando.

En relación al origen de los datos, estimó conveniente explicitar de dónde provienen. Detalló que lo anterior puede realizarse por la vía de la publicación o a través de la consulta que formule el titular.

El Honorable Senador señor Moreira consultó si el encargado de prevención, mencionado en la letra b) del artículo en estudio, puede no existir.

El Presidente de la Comisión, Honorable Senador señor Harboe sostuvo que el modelo de prevención se está creando en la presente iniciativa. Éste constituye un incentivo para que las empresas adopten un modelo preventivo y ello les generará un conjunto de beneficios. Ratificó que no existe la obligación de implementarlo.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena, respondiendo al Honorable Senador señor Harboe, manifestó que el deber de información no impone la obligación de mencionar el origen de los datos, los que en todo caso deben provenir de una fuente autorizada por la ley.

El asesor del Honorable Senador señor Larraín, señor Olmedo, estimó conveniente que se instauren obligaciones de

transparencia activa directa. Constató que pueden surgir problemas respecto a las herramientas de control de la misma. Destacó que no existe la posibilidad de que los ciudadanos puedan iniciar un procedimiento por la infracción de estas obligaciones.

Expresó que en otros cuerpos legales, como en la Ley Orgánica Constitucional de los Partidos Políticos, donde también se regulan obligaciones de transparencia activa, de instancias que no son públicas, se establece un mecanismo de cooperación entre el Consejo para la Transparencia y la respectiva autoridad, para los efectos de homologar estándares y hacer sugerencias y recomendaciones. Connotó que en la iniciativa en estudio hay una desarticulación o escisión con las facultades o la cooperación que podría otorgar el mencionado Consejo. Preguntó cómo se asegura un régimen de control social respecto a las obligaciones detalladas en estas normas.

El asesor del Ministerio de Hacienda, señor Godoy, contestando al Honorable Senador, señor Harboe, en relación a que la regla propuesta solo considera obligaciones de información y transparencia respecto al responsable y no de los encargados, expresó que el encargado puede realizar operaciones de tratamiento por mandato del responsable. Por lo tanto, el titular de datos ejercerá sus derechos siempre respecto del responsable de datos, independiente que las operaciones específicas las realice este último a través de un tercero.

En cuanto a la pregunta del asesor del Honorable Senador Larraín, señor Olmedo, sostuvo que la ley N° 20.285, sobre acceso a la información pública, cautela un bien público distinto al que se resguarda en el ámbito de la protección y tratamiento de datos. Asimismo, indicó que los operadores de un sistema y de otro, son diferentes.

El asesor del Comité Udi, señor Mery, aseveró que la transparencia es deseable, pero estimó que imponerla como un deber no constituye un camino adecuado.

En relación a la posibilidad del control ciudadano, hizo presente que en el artículo 38 bis, ter y quater- que se examinarán más adelante- se establecen sanciones para quienes infringen los deberes que establece esta ley.

En cuanto a la comparación con los partidos políticos, afirmó que existen diferencias, ya que la reciente reforma de la Ley Orgánica Constitucional sobre Partidos Políticos, define a éstos, como asociaciones autónomas y voluntarias organizadas democráticamente, dotadas de personalidad jurídica de derecho público. Recalcó que las mencionadas características no son predicables respecto de los responsables de datos que regula este proyecto de ley.

El Presidente de la Comisión, Honorable Senador señor Harboe precisó que la letra f) del artículo en discusión prescribe: “El derecho que le asiste al titular para solicitar ante el responsable, acceso, rectificación, cancelación, oposición y portabilidad de sus datos personales, de conformidad a esta ley”.

Manifestó que la mencionada letra, circunscribe el ejercicio del derecho a la presente ley. Constató que en el pasado se han dictado algunas normas que les otorgan ciertos derechos a los titulares de datos. Ejemplificó con aquellos que confiere la ley N° 20.575. Dado lo anterior, destacó que lo que no puede ocurrir, es que la obligación de información quede reducida solo a lo que señala la presente normativa.

Sugirió reemplazar la expresión “de conformidad a esta ley”, por: “de conformidad a la ley.”.

Concluido el estudio de esta materia, el señor Presidente de la Comisión sometió a votación el artículo 14 ter propuesto por el Ejecutivo, con la enmienda de agregar las letras f) y g) mencionadas precedentemente y el reemplazo ya indicado.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores De Urresti, Harboe y Moreira, aprobó esta proposición.

Artículo 14 quater

A continuación, la Comisión consideró el artículo 14 quáter que agrega a la ley N° 19.628, una norma que impone al responsable de datos el deber de adoptar medidas de seguridad. Su texto es el siguiente:

“Artículo 14 quater.- Deber de adoptar medidas de seguridad. El responsable de datos debe adoptar las medidas necesarias para resguardar el cumplimiento del principio de seguridad establecido en esta ley, considerando el estado actual de la técnica y los costos de aplicación, junto con la naturaleza, alcance, contexto y fines del tratamiento, así como la probabilidad de los riesgos y la gravedad de sus efectos en relación con el tipo de datos tratados. Las medidas aplicadas por el responsable deben asegurar la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas de tratamiento de datos.

Si las bases de datos que opera el responsable tienen distintos niveles de criticidad deberá adoptar las medidas de seguridad que correspondan al nivel más alto.

Ante la ocurrencia de un incidente de seguridad, y en caso de controversia judicial o administrativa, corresponderá al responsable acreditar la existencia y el funcionamiento de las medidas de seguridad adoptadas en base a los niveles de criticidad y a la tecnología disponible.”.

Asimismo, la Comisión tuvo a la vista el artículo 30 contenido en la Moción parlamentaria que se refunde en este informe. Esta disposición prescribe lo siguiente:

“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.”.

Al iniciarse el estudio de estas disposiciones el grupo de asesores parlamentarios sugirió a la Comisión aprobar el artículo 14 quáter propuesto en el proyecto de ley del Ejecutivo.

El Honorable Senador señor Moreira consultó por el sentido de la expresión “resiliencia”, empleada en la parte final del primer inciso.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena, afirmó que la resiliencia dice relación con la capacidad del sistema que administra el responsable de datos de poder enfrentar problemas y que éstos no afecten su funcionamiento.

El Presidente de la Comisión, Honorable Senador señor Harboe, connotó que dicho término consiste en resistir a determinadas adversidades que se producen en el sistema.

El asesor del Ministerio de Hacienda, señor Godoy, expuso que el texto del Ejecutivo eleva de manera relevante los estándares de seguridad en el tratamiento de datos, lo que constituye una de las cuestiones claves en la mencionada industria. Lo anterior, argumentó, está sujeto a dos elementos importantes que se deben cautelar, a saber, el estado de la técnica y las diferentes medidas de seguridad, dependiendo del nivel de sensibilidad de los datos y el tamaño del responsable.

El Presidente de la Comisión, Honorable Senador señor Harboe, hizo presente que, como se examinará más adelante, la infracción al deber de adoptar medidas de seguridad está calificada como grave.

Concluido el examen de este asunto, el señor Presidente de la Comisión puso en votación el artículo 14 quáter propuesto en el proyecto de ley del Ejecutivo.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores De Urresti, Harboe y Moreira, aprobó el mencionado artículo.

Artículo 14 quinquies

Seguidamente, la Comisión analizó el artículo 14 quinquies del proyecto de ley del Ejecutivo, disposición que agrega a la ley N° 19.628, una norma que establece la obligación del responsable de datos de reportar las vulneraciones a las medidas de seguridad. Su texto es el siguiente:

“Artículo 14 quinquies.- Deber de reportar las vulneraciones a las medidas de seguridad. El responsable de datos debe reportar a la Agencia de Protección de Datos Personales, por los medios más expeditos posibles y sin dilaciones indebidas, las vulneraciones a las medidas de seguridad que ocasionen la destrucción, filtración, pérdida o alteración accidental o ilícita de los datos personales que trate, o la comunicación o acceso no autorizados a dichos datos.

El responsable de datos deberá registrar estas comunicaciones, describiendo la naturaleza de las vulneraciones sufridas, sus efectos, las categorías de datos y el número aproximado de titulares afectados y las medidas adoptadas para gestionarlas y precaver incidentes futuros.

Cuando dichas vulneraciones se refieran a datos personales sensibles o a datos relativos a obligaciones de carácter económico, financiero, bancario o comercial, el responsable deberá también efectuar esta comunicación a los titulares de estos datos. Esta comunicación debe realizarse en un lenguaje claro y sencillo, singularizando los datos afectados, las posibles consecuencias de las vulneraciones de seguridad y las medidas de solución o resguardo adoptadas. La notificación se debe realizar a cada titular afectado y si ello no fuere posible se realizará mediante la difusión o publicación de un aviso en un medio de comunicación social masivo y de alcance nacional.”.

Asimismo, al estudiar este precepto, la Comisión tuvo a la vista lo establecido en el artículo 31, 32 y 33 de la moción parlamentaria que se refunde con el proyecto de ley del Ejecutivo. El texto de dichas disposiciones es el siguiente:

“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, perdida 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 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.”.

Al comenzar el análisis de estas disposiciones, el grupo de asesores parlamentarios sugirió a la Comisión aprobar el artículo 14 quinquies contenido en el proyecto de ley del Ejecutivo, enmendado en los siguientes términos:

“Artículo 14 quinquies.- Deber de reportar las vulneraciones a las medidas de seguridad. El responsable de datos deberá reportar a la Agencia de Protección de Datos Personales, por los medios más expeditos posibles y sin dilaciones indebidas, las vulneraciones a las medidas de seguridad que ocasionen la destrucción, filtración, pérdida o alteración accidental o ilícita de los datos personales que trate o la comunicación o acceso no autorizados a dichos datos, **cuando exista un riesgo razonable que con ocasión de estos incidentes se genere un perjuicio o afectación para los titulares.**

El responsable de datos deberá registrar estas comunicaciones, describiendo la naturaleza de las vulneraciones sufridas, sus efectos, las categorías de datos y el número aproximado de titulares afectados y las medidas adoptadas para gestionarlas y precaver incidentes futuros.

Cuando dichas vulneraciones se refieran a datos personales sensibles o datos relativos a obligaciones de carácter económico, financiero, bancario o comercial, el responsable deberá también efectuar esta comunicación a los titulares de estos datos. Esta comunicación deberá realizarse en un lenguaje claro y sencillo, **individualizando** los datos afectados, las posibles consecuencias de las vulneraciones de seguridad y las medidas de solución o resguardo adoptadas. La notificación se deberá realizar a cada titular afectado y si ello no fuere posible, se realizará mediante la difusión o publicación de un aviso en un medio de comunicación social masivo y de alcance nacional.”.

Seguidamente, **el Presidente de la Comisión, Honorable Senador señor Harboe,** ofreció la palabra **al asesor del Comité Udi, señor Mery**, quien expresó que la redacción del inciso primero, está en términos potenciales. Así se entiende de la lectura de la frase: “cuando exista un riesgo razonable que con ocasión de estos incidentes se genere un perjuicio.”. Consultó al Ejecutivo por el significado de la oración transcrita.

Agregó que en el inciso final se habla de: “un medio de comunicación social masivo de alcance nacional.”. Preguntó si

dicho medio se refiere solo a la prensa escrita o puede ser un soporte web.

El asesor del Ministerio de Hacienda, señor Godoy, respecto a la primera interrogante, constató que con la redacción del inciso primero se trata de evitar un perjuicio efectivo.

En cuanto a la pregunta sobre el medio de comunicación social, sostuvo que éste comprende diversos medios y no solo los escritos.

Puesto en votación el artículo 14 quinquies del Ejecutivo, en los términos propuestos por el grupo de asesores parlamentarios, fue aprobado por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores De Urresti, Harboe y Moreira.

Posteriormente, **el asesor del Ministerio de Hacienda, señor Godoy,** solicitó a la Comisión sustituir, en el inciso tercero, la palabra “individualizando” por “singularizando”.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, De Urresti, Harboe y Larraín, aprobó la enmienda indicada.

Artículo 14 sexies

En seguida, la Comisión consideró el artículo 14 sexies del proyecto de ley del Ejecutivo, disposición que regulará en la ley N° 19.628, la diferenciación de los estándares de cumplimiento. El texto de este precepto es el siguiente:

“Artículo 14 sexies.- Diferenciación de estándares de cumplimiento. Los estándares o condiciones mínimas que se impongan al responsable de datos para el cumplimiento de los deberes de información y de seguridad establecidos en los artículos 14 ter y 14 quáter, respectivamente, serán determinados considerando si el responsable es una persona natural o jurídica; el tamaño de la entidad o empresa de acuerdo a las categorías establecidas en el artículo segundo de la ley N° 20.416, que fija normas especiales para las empresas de menor tamaño, y el volumen y las finalidades de los datos personales que trata.

Los estándares de cumplimiento y las medidas diferenciadas serán especificados en un reglamento dictado por el Ministerio de Hacienda y suscrito por el Ministro o Ministra de Economía, Fomento y Turismo.”.

Al iniciarse el estudio de este precepto, **los representantes del Ejecutivo, señora Piedrabuena y señor Godoy**, presentaron una indicación a la Comisión para aprobar el artículo 14 sexies propuesto por el Ejecutivo, en los siguientes términos:

"Articulo 14 sexies.- Diferenciación de estándares de cumplimiento. Los estándares o condiciones mínimas que se impongan al responsable de datos para el cumplimiento de los deberes de información y de seguridad establecidos en los artículos 14 ter y 14 quáter, respectivamente, serán determinados considerando si el responsable es una persona natural o jurídica, el tamaño de la entidad o empresa de acuerdo a las categorías establecidas en el artículo segundo de la ley N° 20.416, que fija normas especiales para las empresas de menor tamaño, y el volumen y las finalidades de los datos personales que trata.

Los estándares de cumplimiento y las medidas diferenciadas serán especificadas en un reglamento expedido por el Ministerio de Hacienda y suscrito por el Ministro o Ministra de Economía, Fomento y Turismo, **previo informe de la Agencia de Protección de Datos Personales.**

La Agencia de Protección de Datos Personales, al definir los parámetros y mecanismos para determinar los costos derivados del ejercicio de los derechos de acceso y portabilidad de acuerdo al artículo 10 de esta ley, deberá considerar también el volumen de datos, la naturaleza jurídica y el tamaño de la entidad o empresa que tenga la calidad de responsable de datos.".

El Presidente de la Comisión, Honorable Senador señor Harboe consideró que el artículo debe diferenciar entre la pequeña, la mediana y la gran empresa. Consignó que no es posible que se aplique el mismo criterio a todas ellas, sino que hay que tomar en consideración su tamaño.

El Honorable Senador señor Moreira preguntó por qué el reglamento que se menciona en el inciso segundo no es propuesto por la Agencia de Protección de Datos Personales.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena, aseveró que la mencionada Agencia tendrá a su cargo determinar los criterios que se incorporen al reglamento, pero no está facultada para dictarlo.

El Presidente de la Comisión, Honorable Senador señor Harboe recordó que la potestad reglamentaria recae en el Presidente de la República. Sugirió que se indique que la dictación del reglamento se hará escuchando a la Agencia de Protección de Datos.

Además, propuso dictar una norma transitoria que señale que la primera fijación de estándares que contemple el reglamento la realizará el Ministerio de Hacienda conjuntamente con el Ministerio de Economía, Fomento y Turismo.

El asesor del Comité Udi, señor Mery recalcó que se está hablando de estándares que deben ser observados por la industria y por las personas que intervienen en esta actividad. Atendido lo anterior, estimó conveniente que la Agencia tenga una voz preferente. Inquirió qué sucede si las opiniones son diversas entre los mencionados Ministerios y la Agencia.

El Honorable Senador señor Larraín propuso omitir las especificaciones referidas a los ministerios, porque ello constituye una limitación.

El asesor del Ministerio de Hacienda, señor Godoy remarcó que la potestad reglamentaria radica en el Presidente de la República. Sin embargo, los decretos deben ser expedidos a través de un Ministerio. Aseveró que se considera el Ministerio de Economía, porque se reglamentan estándares para empresas de menor tamaño, y dicho Ministerio se relaciona con ellas.

Los incisos primero y tercero fueron aprobados con los votos a favor de los Honorables Senadores señores De Urresti, Harboe y Moreira.

En relación al inciso segundo**, el asesor del Ministerio de Hacienda, señor Godoy**, expresó que el Ejecutivo solicita a la Comisión que recoja el lenguaje inclusivo planteado en esta norma.

Recalcó que el Ejecutivo en las últimas iniciativas presentadas ha persistido en el criterio del lenguaje inclusivo.

El Honorable Senador señor Larraín se mostró contrario incorporar el mencionado lenguaje en la iniciativa**.**

El Presidente de la Comisión, Honorable Senador señor Harboe manifestó que ha motivado la igualdad de género en las empresas públicas y privadas. Sin embargo, demostró su preocupación que la incorporación de dicho lenguaje en el presente texto, pueda servir de base a una interpretación excluyente en otros cuerpos legales, donde no se han incorporado los conceptos inclusivos.

Agregó que la situación se puede salvar si el Ejecutivo lleve a cabo una modificación legal general de inclusión.

Reiteró que hacerlo respecto a la presente iniciativa puede resultar contraproducente en otras áreas donde sí necesitamos mayor equidad e inclusión en materia de género.

El Honorable Senador, señor De Urresti compartió las opiniones antes expresadas**.**

El Honorable Senador señor Larraín complementó lo señalado precedentemente, indicando que en el proyecto de ley que modifica diversos cuerpos legales con el objeto de modernizar el Ministerio de Relaciones Exteriores, se produjo la misma discusión y finalmente, la Comisión de Relaciones Exteriores acordó mantener la redacción tradicional y así lo aprobó la Sala del Senado.

El Presidente de la Comisión, Honorable Senador señor Harboe, declaró cerrado el debate.

Puesta en votación la idea de utilizar la expresión "o Ministra" contenida en el inciso segundo del artículo 14 sexies por el Ejecutivo, fue rechazada, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, De Urresti, Harboe y Larraín.

Este criterio se hizo extensivo a otras disposiciones del proyecto de ley del Ejecutivo que contienen las expresiones tales como: "Ministra" o "Directora". En todas esas disposiciones se resolvió utilizar el término "Ministro" o "Director", según corresponda.

Resuelto lo anterior**, el señor Presidente de la Comisión puso en votación el inciso segundo.**

Esta disposición fue aprobada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Araya, Harboe y Larraín.

Artículo 15

A continuación, la Comisión analizó la enmienda que se propone al artículo 15 de la ley N° 19.628, disposición que establece causales por las que no podrá solicitarse información, modificación, cancelación o bloqueo de datos.

En relación con este precepto, el proyecto de ley del Ejecutivo propone sustituir tal precepto por el siguiente:

“Artículo 15.- Cesión o transferencia de bases de datos personales. Se podrán ceder todo o parte de las bases de datos personales que disponga o administre el responsable de datos cuando la cesión sea necesaria para cumplir con los fines del tratamiento o las funciones del cedente o del cesionario, de conformidad con las disposiciones de esta ley.

La cesión de datos personales requiere el consentimiento previo del titular a quien conciernen los datos, salvo las excepciones legales.

En caso que el consentimiento otorgado por el titular al momento de realizarse la recolección de los datos personales no haya considerado la cesión de los mismos, éste debe recabarse antes que se produzca, considerándose para todos los efectos legales como una nueva operación de tratamiento.

Con el objeto que el titular preste su consentimiento a la cesión, el responsable debe entregar la información necesaria que le permita conocer la finalidad a la cual se destinarán los datos y el tipo de actividades que realiza el cesionario.

La cesión de datos debe constar por escrito o a través de cualquier medio electrónico idóneo. En ella se deberá individualizar a las partes, las bases de datos que son objeto de la cesión, las finalidades previstas para el tratamiento y los demás antecedentes o estipulaciones que acuerden el cedente y el cesionario.

El tratamiento de los datos personales cedidos debe realizarse por el cesionario de conformidad a las finalidades establecidas en el contrato de cesión.

Una vez perfeccionada la cesión, el cesionario adquiere la condición de responsable de datos para todos los efectos legales, respecto de las bases de datos que fueron objeto de la cesión. El cedente, por su parte, también mantiene la calidad de responsable de datos respecto de las operaciones de tratamiento que continúe realizando.

Si se verifica una cesión de datos sin contar con el consentimiento del titular, siendo éste necesario, o sin informarle acerca de la finalidad a la cual serán destinados los datos cedidos o el tipo de actividades que desarrolla el cesionario, la cesión será considerada nula para todos los efectos legales, debiendo el cesionario cancelar todos los datos recibidos, sin perjuicio de las responsabilidades legales que correspondan.

A las cesiones de datos anonimizados no le son aplicables las reglas señaladas en este artículo.”.

En relación con este precepto, la Comisión tuvo también a la vista la norma contenida en el artículo 7° de la moción parlamentaria que se refunde en este informe. Este precepto dispone lo siguiente:

“Artículo 7°. 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 que 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.”.

Al iniciarse el estudio de estas disposiciones, los representantes del Ejecutivo sugirieron a la Comisión aprobar el proyecto de ley del Gobierno, enmendado en los siguientes términos:

“Artículo 15.- Cesión de datos personales. Los datos personales podrán ser cedidos con el consentimiento del titular y para el cumplimiento de los fines del tratamiento. También se podrán ceder los datos personales cuando la cesión sea necesaria para la ejecución de un contrato en que es parte el titular; cuando exista un interés legítimo del

cedente o del cesionario, en los términos previstos en la letra e) del artículo 13, y cuando lo disponga la ley.

En caso que el consentimiento otorgado por el titular al momento de realizarse la recolección de los datos personales no haya considerado la cesión de los mismos, éste debe recabarse antes que se produzca, considerándose para todos los efectos legales como una nueva operación de tratamiento.

La cesión de datos deberá constar por escrito o a través de cualquier medio electrónico idóneo. En ella se deberá individualizar a las partes, los datos que son objeto de la cesión, las finalidades previstas para el tratamiento y los demás antecedentes o estipulaciones que acuerden el cedente y el cesionario.

El tratamiento de los datos personales cedidos deberá realizarse por el cesionario de conformidad a las finalidades establecidas en el contrato de cesión.

Una vez perfeccionada la cesión, el cesionario adquiere la condición de responsable de datos para todos los efectos legales. El cedente, por su parte, también mantiene la calidad de responsable de datos, respecto de las operaciones de tratamiento que continúe realizando.

Si se verifica una cesión de datos sin contar con el consentimiento del titular, siendo éste necesario, la cesión será considerada nula para todos los efectos legales, debiendo el cesionario cancelar todos los datos recibidos, sin perjuicio de las responsabilidades legales que correspondan.”.

Seguidamente, **el asesor del Ministerio de Hacienda, señor Godoy,** hizo presente que todas las operaciones que efectúa un responsable de datos constituyen tratamiento. Añadió que la única actividad que queda excluida del mencionado procedimiento, es la cesión. Por lo tanto, desde el punto de vista de su regulación, la norma en estudio, establece que para que un responsable ceda los datos a otro, debe contar con el consentimiento del titular o con alguna fuente de legitimidad.

El Presidente de la Comisión, Honorable Senador señor Harboe constató que la cesión es una operación económica que se realiza diariamente. Preguntó por la situación en que quedan los datos cuando se vende la empresa que realiza el tratamiento de ellos. Consultó por el grado de responsabilidad del cedente, al transferir los datos a un cesionario que no se dedica al tratamiento. Asimismo, inquirió por la situación en que un titular ha dado el consentimiento mediante un contrato de

adhesión, y posterior a ello se produce la cesión de los datos o la venta de la empresa.

El asesor del Ministerio de Hacienda, señor Godoy, señaló que esta iniciativa intenta normar aquellos intercambios de bases de datos que no se encuentran regulados. Aseveró que para efectos de la cesión de datos, no es suficiente la base de licitud del tratamiento, sino que hay que contar con una adicional.

Añadió que los criterios que dan legitimidad a las cesiones de datos son: el consentimiento, el contrato y el interés legítimo.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena, ratificó que para ceder los datos se requiere el consentimiento del titular. Precisó que en el caso en que se cedan los datos entre dos responsables, el cedente tiene que transferirlos con el mencionado consentimiento. Aseveró que la base de datos solo puede transferirse para ser utilizada con el mismo fin para el cual se entregó originalmente.

El Presidente de la Comisión, Honorable Senador señor Harboe, preguntó por la situación en que el cesionario carece de las medidas internas de protección.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena, constató que el cesionario se convierte en responsable por el hecho de la cesión.

El Honorable Senador señor De Urresti estimó oportuno establecer la responsabilidad solidaria respecto del cedente.

El Presidente de la Comisión, Honorable Senador señor Harboe propuso que se tome en consideración la circunstancia de que exista una diferencia ostensible entre el titular de datos y el responsable.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena, expresó que si el consentimiento fue recabado en contexto de desigualdad ostensible, éste no sería válido y mantendría dicho estado al momento de la cesión.

El asesor del Comité Udi, señor Mery consultó si el cedente podría retener la información esencial que contienen los datos. Subrayó que el concepto de cesión no necesariamente implica que este último tenga que eliminar los datos que tiene en su poder.

Agregó que en el inciso final se emplea la expresión: “la cesión será considerada nula para todos los efectos legales”.

Estimó innecesario utilizar la locución “para todos los efectos legales”, ya que constituye una redundancia.

Sugirió, también en el último inciso reemplazar el término “cancelar”, por “suprimir”.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena, respondiendo al señor Mery, precisó que cuando se ceden los datos, el cedente mantiene la información en su poder. Por lo anterior, el cedente sigue siendo responsable. Respecto a la sugerencia del señor Mery, se mostró de acuerdo en utilizar la palabra suprimir.

El Presidente de la Comisión, Honorable Senador señor Harboe, constató que si se filtra un dato, tanto cedente como cesionario pueden responsabilizarse mutuamente de aquello.

Consultó la utilidad de que el cedente mantenga una copia de la información, si el objetivo de la cesión es endosar la responsabilidad al cesionario.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena, ejemplificó, señalando que una empresa pida los datos a una persona para enviarle una cuenta, pero asimismo, ésta los puede utilizar para encargar un estudio de mercado a una empresa distinta. Precisó que en el caso descrito estamos ante una cesión de base de datos, en que la información es conservada por el cedente.

Estimó pertinente que los datos los conserve el cedente, siempre que cuente con el consentimiento y una fuente de legitimidad.

El Presidente de la Comisión, Honorable Senador señor Harboe consultó qué sucede en caso de venta de una empresa.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena, aseveró que en la situación planteada, la empresa adquirente, no puede comprar la base de datos, a menos que sean del mismo rubro, o que se pueda aplicar la causa de licitud del interés legítimo.

El asesor del Ministerio de Hacienda, señor Godoy, consignó que el texto señala expresamente que el cedente mantiene la responsabilidad, respecto de los tratamientos que sigan efectuando.

En relación a lo consultado por el Honorable Senador, señor De Urresti, constató que el artículo 10, otorga la posibilidad de que el titular recurra ante cualquiera de los responsables.

Puesto en votación el artículo 15 del Ejecutivo, fue aprobado con las enmiendas indicadas precedentemente, por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores De Urresti, Harboe y Moreira.

Artículo 15 bis

Seguidamente, la Comisión analizó la propuesta del proyecto de ley del Ejecutivo que sugiere regular el tratamiento de datos efectuado por un tercero o mandatario. Su texto es el siguiente:

"Artículo 15 bis.- Tratamiento de datos por parte de un tercero o mandatario. El responsable puede efectuar el tratamiento de datos en forma directa o a través de un tercero mandatado para este efecto. En este último caso, el tercero o mandatario realiza el tratamiento de datos personales conforme al encargo y a las instrucciones que le imparta el responsable, quedándole prohibido su tratamiento, cesión o entrega para un objeto distinto del convenido con el responsable.

Si el tercero trata, cede o entrega los datos o la base de datos con un objeto distinto del encargo convenido o a una persona distinta del responsable, se le considerará como responsable de datos para todos los efectos legales, debiendo responder solidariamente por las infracciones y los perjuicios en que hubiere incurrido, sin perjuicio de las responsabilidades contractuales que le correspondan frente al responsable de datos.

Cumplida la prestación del servicio de tratamiento por parte del tercero, los datos que obran en su poder deben ser cancelados o devueltos al responsable de datos, según corresponda.".

Asimismo, la Comisión tuvo a la vista lo que dispone el artículo 29 contenido en la moción parlamentaria que se refunde en este informe. Su texto es el siguiente:

"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 regirá 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 estipulara, 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;

e) 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.”.

Al iniciarse el estudio de estos preceptos, el grupo de asesores parlamentarios sugirió a la Comisión aprobar la norma propuesta por el Ejecutivo, enmendada en los siguientes términos:

“Artículo 15 bis.- Tratamiento de datos a través de un tercero mandatario o encargado. El responsable puede efectuar el tratamiento de datos en forma directa o a través de un tercero mandatario o encargado. En este último caso, el tercero mandatario o encargado realiza el tratamiento de datos personales conforme al encargo y a las instrucciones que le imparta el responsable, quedándole prohibido su tratamiento, cesión o entrega para un objeto distinto del convenido con el responsable.

Si el tercero **mandatario o encargado** trata, cede o entrega los datos con un objeto distinto del encargo convenido, se le considerará como responsable de datos para todos los efectos legales, debiendo responder solidariamente por las infracciones y los perjuicios en que incurra, sin perjuicio de las responsabilidades contractuales que le correspondan frente al responsable de datos.

El tratamiento de datos a través de un tercero mandatario o encargado se regirá por el contrato celebrado entre el responsable y el encargado, con arreglo a la legislación vigente. En el contrato se deberá establecer el objeto del encargo, la duración del mismo, la finalidad del tratamiento, el tipo de datos personales tratados, las categorías de titulares a quienes conciernen los datos, y los derechos y obligaciones de las partes. La Agencia de Protección de Datos Personales en su página web pondrá a disposición del público modelos tipo de contratos.

El tercero mandatario o encargado deberá cumplir con lo dispuesto en los artículos 14 quater y 14 quinquies.

Cumplida la prestación del servicio de tratamiento por parte del tercero **mandatario o encargado**, los datos que obran en su poder deben ser cancelados o devueltos al responsable de datos, según corresponda.

Las personas naturales o jurídicas que presten servicios de infraestructura, plataforma, software u otros servicios para el almacenamiento o procesamiento de los datos, o para facilitar enlaces o instrumentos de búsqueda, no tendrán la calidad de responsable de datos para los efectos de esta ley, salvo que tomen

decisiones acerca de los medios o fines del tratamiento de datos, en cuyo caso responderán de acuerdo a las normas previstas en esta ley para los responsables de datos, sin perjuicio de las demás responsabilidades y sanciones que les puedan caber por incumplimiento de contratos o infracciones legales.”.

Respecto a esta disposición, **la asesora del Ministerio de Economía, señora Bernardita Piedrabuena,** precisó que era necesario agregar en el inciso cuarto, a continuación de la palabra “artículos”, la expresión “14 bis,”. Aclaró que el mencionado artículo se refiere al deber de secreto y confidencialidad.

Precisó que en el inciso final debe decirse: “medios y fines”, en lugar de “medios o fines”.

Seguidamente, **el asesor del Comité Udi, señor Mery,** indicó que en el inciso segundo se habla de responder solidariamente por las infracciones y los perjuicios. Hizo presente que de las infracciones se responde directamente, no solidariamente.

Puesto en votación el artículo 15 bis, fue aprobado con las enmiendas señaladas, por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores, señores De Urresti, Harboe y Moreira.

En una sesión posterior, los representantes del Ejecutivo, señora Piedrabuena y señor Godoy, propusieron a la Comisión sustituir el inciso segundo por el siguiente:

“Si el tercero mandatario o encargado trata, cede o entrega los datos con un objeto distinto del encargo convenido, se le considerará como responsable de datos para todos los efectos legales, debiendo responder por las infracciones en que incurra y por los daños que ocasione, sin perjuicio de las responsabilidades contractuales que le correspondan frente al responsable de datos.”.

El Presidente de la Comisión, Honorable Senador señor Harboe señaló que el mandante le encarga a un mandatario que realice un conjunto de gestiones, y éste las lleva a cabo vulnerando la ley. La disposición hace responsable a este último. Connotó que en el ámbito del derecho público, el mandante no cede su responsabilidad.

Recomendó que el mandante sea solidariamente responsable, con la finalidad que adopte medidas preventivas y exija un código de conducta adecuado a su mandatario.

El asesor del Ministerio de Hacienda, señor Godoy hizo presente que el inciso primero del artículo 10 dispone lo siguiente:

"Artículo 10.- Forma y medios de ejercer los derechos del titular de datos. Los derechos reconocidos en esta ley se ejercen por el titular ante el responsable de datos. Si los datos personales del titular son tratados por diversos responsables, el titular puede ejercer sus derechos ante cualquiera de ellos.".

Agregó que para el titular, el responsable es el que realice el tratamiento de datos. Aseveró que el titular siempre tiene la posibilidad de accionar en contra del responsable. Si existe pluralidad de responsables, podrá dirigirse en contra de cualquiera de ellos.

El Presidente de la Comisión, Honorable Senador señor Harboe, observó que en la última hipótesis planteada se habla de más de un responsable. Sin embargo, constató que el caso plasmado en el inciso segundo del artículo 15 bis, es distinto. Se refiere a la situación en que un responsable le ha encomendado el tratamiento de datos a un mandatario y este último será el que debe responder ante el titular.

Afirmó que en la última situación descrita, el mandante también debe resultar obligado solidariamente.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena, consignó que se ha definido responsable como aquel que decide sobre los fines y los medios del tratamiento de datos.

Añadió que un tercero que no ejecutó el mandato en la forma debida, debe asumir la responsabilidad respectiva. Asimismo, el mandante resulta obligado solidariamente.

El Presidente de la Comisión, Honorable Senador señor Harboe, reiteró que si de la mera lectura del artículo 10 se pudiese colegir que el mandatario es considerado responsable, no tiene sentido especificarlo en el artículo en discusión.

Recalcó que en el artículo 10 solo se sitúa en el caso de la existencia de múltiples responsables. Por su parte, en el artículo 15 bis, hace referencia a la figura del mandato y las responsabilidades que le caben al mandante y al mandatario.

El asesor del Ministerio de Hacienda, señor Godoy, señaló que con la propuesta del artículo 15 bis se está configurando responsabilidad directa del tercero y que tanto mandante como mandatario resultan obligados ante un incumplimiento del encargado de desarrollar la

gestión correspondiente. Sugirió introducir el término “solidario” para una mayor claridad de la norma.

El Presidente de la Comisión, Honorable Senador señor Harboe consideró clave incorporar ese término. Recordó que la responsabilidad solidaria solo tiene fuente legal.

Concluido el debate, el señor Presidente de la Comisión, puso en votación, a sugerencia del Ejecutivo, la siguiente redacción:

“Si el tercero mandatario o encargado trata, cede o entrega los datos con un objeto distinto del encargo convenido, se le considerará como responsable de datos para todos los efectos legales, debiendo responder por las infracciones en que incurra y solidariamente por los daños que ocasione, sin perjuicio de las responsabilidades contractuales que le correspondan frente al mandante o responsable de datos.”.

Esta disposición fue aprobada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Araya, De Urresti, Harboe y Larraín.

Artículo 15 ter

A continuación la Comisión consideró la proposición del Ejecutivo para incorporar a la ley N° 19.628, un artículo nuevo que dispone lo siguiente:

“Artículo 15 ter.- Tratamiento automatizado de grandes volúmenes de datos.- El responsable de datos puede establecer procedimientos automatizados de tratamiento y de transferencia de grandes volúmenes de datos, siempre que éstos cautelen los derechos del titular y el tratamiento guarde relación con las finalidades de las personas o entidades participantes.

El titular de datos tiene derecho a solicitar al responsable que ninguna decisión que le afecte de manera significativa se adopte exclusivamente basada en el tratamiento automatizado de sus datos, salvo que sea necesario para la celebración o ejecución de un contrato entre el titular y el responsable, exista consentimiento previo y explícito del titular o lo disponga la ley.”.

Al iniciarse su estudio, **los representantes del Ejecutivo, señora Piedrabuena y señor Godoy,** indicaron que esta disposición no se debía acoger ya que su contenido está considerado en la nueva redacción del artículo 8° bis.

Constató que en el artículo antes mencionado se realiza una construcción más sólida e integral que recoge tanto los tratamientos automatizados como la posibilidad que las personas, frente a estos tratamientos puedan impugnar las decisiones que allí se adopten y puedan requerir intervención humana en esos procesos.

El Presidente de la Comisión, Honorable Senador señor Harboe aseveró que estamos ante dos caras del mismo procedimiento. Precisó que el artículo 8 bis dice relación con el derecho del titular de datos frente al tratamiento automatizado. Sin embargo, en el artículo 15 ter se construye la fuente legal para que una empresa pueda realizar el tratamiento automatizado.

Recalcó que ambas disposiciones no son contradictorias. Las dos deben coexistir.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena apuntó que el inciso segundo del artículo 15 ter debe eliminarse, porque está recogido en el artículo 8 bis.

El Presidente de la Comisión, Honorable Senador señor Harboe se mostró partidario de no suprimir el inciso primero.

Relató el caso de una empresa que quiere desarrollar un negocio de tratamiento automatizado de datos para construir perfiles. Ésta inicia su actividad y un titular decide ejercer el derecho de oposición y se da cuenta en el camino que no hay fuente legal para que exista ese tratamiento.

Ante lo anterior, sugirió permitir que se pueda llevar a cabo ese tipo de negocio, pero éste se realice con respeto a los derechos de los titulares.

Destacó que está en el fundamento del proyecto que si estamos consignando legalmente una determinada actividad, las fuentes deben ser legítimas.

El Honorable Senador, señor Larraín suscribió lo planteado por el Honorable Senador señor Harboe.

Estimó que las ideas contenidas en el inciso primero del artículo 15 ter, no están recogidas plenamente en el 8° bis. Expresó que el artículo 15 ter cautela los derechos de los titulares que buscan asegurar que no resulten perjudicados por el tratamiento de grandes volúmenes de datos.

Atendido lo expuesto, **el Presidente de la Comisión, Honorable Senador señor Harboe,** sugirió conservar el inciso primero del artículo 15 ter y eliminar su inciso segundo.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó el inciso primero del artículo 15 ter propuesto por el Ejecutivo, con enmiendas de forma, y eliminó el inciso segundo.

Artículo 16

A continuación, la Comisión trató la modificación al artículo 16 de la ley N° 19.628.

Esta disposición establece que si el responsable del registro o banco de datos no se pronuncia sobre la solicitud del requirente dentro de dos días hábiles, o 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 del domicilio del responsable, que se encuentre de turno según las reglas correspondientes, solicitando amparo a los derechos consagrados en el artículo precedente.

Agrega que el procedimiento se sujetará a las reglas siguientes:

a) La reclamación señalará claramente la infracción cometida y los hechos que la configuran, y deberá acompañarse de los medios de prueba que los acrediten, en su caso.

b) El tribunal dispondrá que la reclamación sea notificada por cédula, dejada en el domicilio del responsable del banco de datos correspondiente. En igual forma se notificará la sentencia que se dicte.

c) El responsable del banco de datos deberá presentar sus descargos dentro de quinto día hábil y adjuntar los medios de prueba que acrediten los hechos en que los funda. De no disponer de ellos, expresará esta circunstancia y el tribunal fijará una audiencia, para dentro de quinto día hábil, a fin de recibir la prueba ofrecida y no acompañada.

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.

Añade que 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.

Luego, precisa que 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 podrá aplicar una multa de una a diez unidades tributarias mensuales, o de diez a cincuenta unidades tributarias mensuales si se tratare de una infracción a lo dispuesto en los artículos 17 y 18.

Concluye señalando que la falta de entrega oportuna de la información o el retardo en efectuar la modificación, en la forma que decrete el Tribunal, serán castigados con multa de dos a cincuenta unidades tributarias mensuales y, si el responsable del banco de

datos requerido fuere un organismo público, el tribunal podrá sancionar al jefe del Servicio con la suspensión de su cargo, por un lapso de cinco a quince días.

En relación a esta disposición, el proyecto de ley del Ejecutivo sustituye esta disposición por otra que textualmente establece lo siguiente:

"Párrafo Segundo
Del tratamiento de los datos personales sensibles

Artículo 16.- Regla general para el tratamiento de datos personales sensibles. El tratamiento de los datos personales sensibles sólo puede realizarse cuando el titular a quien conciernen estos datos preste su consentimiento libre e informado, otorgado previamente, para un tratamiento específico y lo manifieste en forma expresa a través de una declaración escrita, verbal o por un medio tecnológico equivalente.

No obstante lo anterior, no se requiere el consentimiento del titular en los siguientes casos:

a) Cuando el tratamiento se refiere a datos personales sensibles que el titular ha hecho manifiestamente públicos.

b) Cuando el tratamiento es realizado por una fundación, una asociación o cualquier otra entidad que no persiga fines de lucro, cuya finalidad sea política, filosófica, religiosa, cultural, deportiva, sindical o gremial, siempre que el tratamiento que realicen se refiera exclusivamente a sus miembros o afiliados, tenga por objeto cumplir sus finalidades específicas, la entidad otorgue las garantías necesarias para evitar un uso o tratamiento no autorizado, y los datos no se comuniquen o cedan a terceros. Cumpliéndose todas estas condiciones, las entidades señaladas no requerirán el consentimiento de los titulares para tratar sus datos personales, incluidos sus datos sensibles. En caso de duda o controversia administrativa o judicial, el responsable de datos deberá acreditar que el tratamiento realizado cumple con los requisitos anteriores.

c) Cuando el tratamiento de los datos personales, incluidos los datos relativos a la salud del titular, resulte indispensable para salvaguardar la vida, salud o integridad física o psíquica del titular o de otra persona, o cuando el titular se encuentre física o jurídicamente impedido de otorgar su consentimiento. Una vez que cese el impedimento, el responsable debe informar detalladamente al titular los datos que fueron tratados y las operaciones específicas de tratamiento que fueron realizadas.

d) Cuando el tratamiento de datos personales sensibles lo autoriza o mandata expresamente la ley.".

Al iniciarse el estudio de este precepto, la Comisión tuvo a la vista lo establecido en el artículo 9° de la Moción Parlamentaria que se refunde en este informe. Su texto es el siguiente:

“Artículo 9°. 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 fondón 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.”.

Por su parte, el grupo de asesores parlamentarios sugirió a la Comisión aprobar el artículo 16 del proyecto de ley del Ejecutivo, enmendado en los siguientes términos:

“Párrafo Segundo
Del tratamiento de los datos personales sensibles

Artículo 16.- Regla general para el tratamiento de datos personales sensibles. El tratamiento de los datos personales sensibles sólo puede realizarse cuando el titular a quien conciernen estos datos **manifiesta** su consentimiento en forma expresa, otorgado a través de una declaración escrita, verbal o por un medio tecnológico equivalente.

Es lícito el tratamiento de datos personales sensibles, sin el consentimiento del titular, en los siguientes casos:

a) Cuando el tratamiento se refiere a datos personales sensibles que el titular ha hecho manifiestamente públicos **y su tratamiento esté relacionado con los fines para los cuales fueron publicados**.

b) **Cuando el tratamiento se basa en un interés legítimo realizado por una fundación, una asociación o cualquier otra entidad que no persiga fines de lucro, cuya finalidad sea política, filosófica, religiosa, cultural, sindical o gremial, siempre que el tratamiento que realicen se refiera exclusivamente a sus miembros o afiliados, tenga por objeto cumplir sus finalidades específicas, la entidad otorgue las garantías necesarias para evitar un uso o tratamiento no autorizados, y los datos no se comuniquen o cedan a terceros. En caso de duda o controversia administrativa o judicial, el responsable de datos deberá acreditar que el tratamiento realizado cumple con los requisitos anteriores.**

c) Cuando el tratamiento de los datos personales, incluidos los datos relativos a la salud del titular, resulte indispensable para salvaguardar la vida, salud o integridad física o psíquica del titular o de otra persona o, cuando el titular se encuentre física o jurídicamente impedido de otorgar su consentimiento. Una vez que cese el impedimento, el responsable debe informar detalladamente al titular los datos que fueron tratados y las operaciones específicas de tratamiento que fueron realizadas.

d) Cuando el tratamiento de los datos sea necesario para la formulación, ejercicio o defensa de un derecho ante los tribunales de justicia.

e) Cuando el tratamiento de datos sea necesario para el ejercicio de derechos y el cumplimiento de obligaciones del responsable o del titular de datos, en el ámbito laboral o de seguridad social, y se realice en el marco de la ley.

f) Cuando el tratamiento de datos personales sensibles lo autorice o mandate expresamente la ley.".

Presentados estos antecedentes, **el Presidente de la Comisión, Honorable Senador señor Harboe,** manifestó que esta disposición exige el consentimiento expreso, escrito o verbal, o por un medio tecnológico equivalente. Sin embargo, resaltó, no incorpora un requisito que sí se incluye en la Moción, a saber, que éste debe ser previo. Con ello se quiere evitar que el consentimiento se preste tardíamente. Es decir, una vez iniciado el tratamiento de los datos.

El asesor del Ministerio de Hacienda, señor Godoy, expresó que la voluntad del titular, independiente de la oportunidad en que se dicte, tiene la posibilidad de otorgarle licitud a un tratamiento, aunque los datos hayan sido recolectados con anterioridad.

El asesor del Comité Udi, señor Mery hizo presente una duda respecto a la letra b) del artículo en estudio. Específicamente cuando se señala: "…fundación, una asociación o cualquier otra entidad que no persiga fines de lucro…". Hizo presente que la expresión "entidad" es muy amplia y consideró deseable que se precisara.

El asesor del Ministerio de Hacienda, señor Godoy, sostuvo que se intentó incorporar una denominación que pudiese incluir otras organizaciones sin fines de lucro, que no necesariamente participen de la naturaleza jurídica de una fundación o asociación.

El asesor del Comité Udi, señor Mery enfatizó que se debe asegurar que nadie puede excusarse con el argumento que carece de personalidad jurídica.

El asesor del Ministerio de Hacienda, señor Godoy, destacó que cuesta encontrar un caso de una entidad que realice tratamiento de datos sensibles y que carezca de personalidad jurídica.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena, manifestó que cualquier otra asociación, que carezca de personalidad jurídica, si desea tratar datos personales sensibles, deberá obtener el consentimiento del titular de los datos y éste, además, deberá ser expreso.

El Presidente de la Comisión, Honorable Senador señor Harboe insistió que el consentimiento a que hace alusión el inciso primero del artículo 16, sea "previo".

El asesor del Comité Udi, señor Mery constató que si el consentimiento no fuese previo, el tratamiento sería ilícito. Se mostró contrario a dicha posibilidad.

En esta parte del debate, **el asesor del Ministerio de Hacienda, señor Godoy** propuso reemplazar, la letra b), por la siguiente:

"b) Cuando el tratamiento se basa en un interés legítimo realizado por una persona jurídica de derecho público o de derecho privado que no persiga fines de lucro y se cumplan las siguientes condiciones: i.- su finalidad sea política, filosófica, religiosa, cultural, sindical o gremial; ii.- el tratamiento que realice se refiera exclusivamente a sus miembros o afiliados; iii.- el tratamiento de datos tenga por objeto cumplir las finalidades específicas de la institución; iv.- la persona jurídica otorgue las garantías necesarias para evitar un uso o tratamiento no autorizado de los datos, y v.- los datos personales no se comuniquen o cedan a terceros. Cumpliéndose estas condiciones, la persona jurídica no requerirá el consentimiento del titular para tratar sus datos, incluidos los datos personales sensibles. En caso de duda o controversia administrativa o judicial, el responsable de datos deberá acreditar su concurrencia."

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena manifestó que la propuesta ordena las mismas condiciones ya conocidas por la Comisión, y realiza una modificación relevante. Ésta última consiste en que si se observan las condiciones señaladas, no se requerirá el consentimiento del titular para el tratamiento de datos no sensibles y sensibles.

El Honorable Senador señor Larraín advirtió que estamos en la hipótesis en que el titular de los datos pertenece a una determinada organización. Estimó complejo que esta última pueda disponer de los datos sensibles y no sensibles de sus asociados.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena subrayó que hay que situarse en el contexto de los datos sensibles. Agregó que la ley establece que éstos pueden ser tratados cuando ha existido consentimiento expreso del titular, y en algunos casos, bajo ciertas circunstancias.

Sostuvo que ser miembro de una asociación constituye un dato sensible.

El Presidente de la Comisión, Honorable Senador señor Harboe consignó que la divulgación de los datos sensibles puede generar un grave daño. Por lo tanto, la norma debe ser más rigurosa.

Ejemplificó con el caso de una persona que pertenece a un partido político determinado y éste no anonimiza su militancia y es publicada.

Recordó que en la estructura de la presente iniciativa, el dato sensible es el que más se intenta proteger. Consideró que la disposición que propone el Ejecutivo es bastante laxa.

El asesor del Ministerio de Hacienda, señor Godoy, insistió que la norma en estudio viene a tratar de resolver una cuestión práctica que ocurre con mucha frecuencia.

Aseveró que la afiliación política y sindical; la pertenencia a un credo religioso constituyen datos sensibles. Afirmó que éstos no cuentan con una protección eficaz.

Añadió que en el caso de haber un uso indebido de estos datos se configurará una infracción gravísima.

El Presidente de la Comisión, Honorable Senador señor Harboe remarcó que al hablar de dato sensible, debe circunscribirse la sensibilidad del mismo, de acuerdo a la naturaleza de la organización. Agregó que puede ocurrir que una iglesia no solo tenga acceso a datos sensibles propios de la adscripción del credo de sus feligreses.

El Honorable Senador señor Larraín precisó que uno de los requisitos que establece la disposición consiste en que los datos no se comuniquen o cedan a terceros.

Preguntó cómo se pueden usar los datos, si éstos no se pueden comunicar.

El asesor del Ministerio de Economía, señor Braulio Palma, sostuvo que ciertas organizaciones sociales comunitarias utilizan información. Un ejemplo lo constituye el caso de una junta de vecinos que realiza un paseo con menores de edad y uno de ellos puede presentar una afección de salud. Ese dato puede ser recopilado por la mencionada organización y podrá ser utilizado si es que ocurre alguna emergencia.

Subrayó que con la norma se intenta elevar el estándar del tratamiento y la protección de los datos personales. Agregó que no se debe someter, en especial a las organizaciones de la sociedad civil, a un nivel de estándar muy alto.

El Presidente de la Comisión, Honorable Senador señor Harboe consultó cómo se asegura la anonimización de los datos cuando la persona deja de pertenecer a una determinada asociación.

Insistió en que la divulgación de los datos sensibles puede ocasionar un daño irreparable.

El asesor del Ministerio de Hacienda, señor Godoy, hizo presente que tanto en la legislación vigente, como en la reglamentación europea, existe una norma similar.

Propuso complementar la norma en el siguiente sentido: “Producida la desafiliación del miembro de la organización, ésta deberá proceder a la anonimización o cancelación de los datos.”.

El Presidente de la Comisión, Honorable Senador señor Harboe declaró cerrado el debate.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó con la enmienda consignada en la nueva letra b) propuesta por el Ejecutivo.

Las demás disposiciones contenidas en el artículo 16 fueron aprobadas por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores De Urresti, Harboe y Moreira.

Artículo 16 bis

A continuación, la Comisión trató el artículo 16 bis del proyecto de ley del Ejecutivo que incorpora un artículo nuevo a la ley N° 19.628, disposición que regula el régimen jurídico para tratar los datos relativos a la salud de una persona. Su texto es el siguiente:

“Artículo 16 bis.- Datos personales relativos a la salud. Los datos personales relativos a la salud del titular sólo pueden ser objeto de tratamiento cuando sean necesarios para el diagnóstico de una enfermedad o para la determinación de un tratamiento médico, siempre que el diagnóstico o el tratamiento, según corresponda, se realicen por establecimientos de salud públicos o privados o por un profesional de la salud titular del secreto profesional o por otra persona sujeta a una obligación equivalente de secreto, establecido en la ley o en un contrato.

También es lícito el tratamiento de los datos personales relativos a la salud del titular, en los siguientes casos:

a) Cuando exista una urgencia médica o sanitaria declarada por la autoridad.

b) Cuando se deba calificar el grado de dependencia o discapacidad de una persona.

c) Cuando resulte indispensable para la ejecución o cumplimiento de un contrato cuyo objeto o finalidad exija tratar datos relativos a la salud del titular.

d) Cuando sean utilizados con fines históricos, estadísticos o científicos, para estudios o investigaciones que atiendan fines de interés público o vayan en beneficio de la salud humana o para el desarrollo de productos o insumos médicos que no podrían desarrollarse de otra manera.”.

Al iniciarse el estudio de esta disposición, el grupo de asesores parlamentarios sugirió a la Comisión aprobar el precepto del Ejecutivo, enmendado en los siguientes términos.

“Artículo 16 bis.- Datos personales relativos a la salud. **Cumpliéndose lo dispuesto en el artículo 16, los datos personales relativos a la salud del titular sólo pueden ser tratados en los siguientes casos:**

a) Cuando sea necesario para el diagnóstico de una enfermedad o para la determinación de un tratamiento médico, siempre que el diagnóstico o el tratamiento, según corresponda, se realicen por un establecimiento de salud o por un profesional de la salud.

b) Cuando exista una urgencia médica o sanitaria.

c) Cuando se deba calificar el grado de dependencia o discapacidad de una persona.

d) Cuando resulte indispensable para la ejecución o cumplimiento de un contrato cuyo objeto o finalidad exija tratar datos relativos a la salud del titular.

e) Cuando sean utilizados con fines históricos, estadísticos o científicos, para estudios o investigaciones que atiendan fines de interés público o vayan en beneficio de la salud humana, o para el desarrollo de productos o insumos médicos que no podrían desarrollarse de otra manera.

El resultado de los estudios e investigaciones científicas que utilicen datos personales relativos a la salud pueden ser

publicados o difundidos libremente, debiendo previamente anonimizarse los datos que se publiquen.”.

En relación a estas propuestas, **el Presidente de la Comisión, Honorable Senador señor Harboe,** afirmó que esta disposición se debe estudiar conjuntamente con la ley N° 20.584, que regula los derechos y deberes que tienen las personas en relación con acciones vinculadas a su atención en salud.

Seguidamente, **la asesora del Ministerio de Economía, señora Piedrabuena**, precisó que la letra c) de este artículo dice relación con la evaluación de los programas de subsidio, ya que en ellos se otorga un mayor puntaje en caso de dependencia psicológica o discapacidad. Dado la importancia de lo anterior, se exime de prestar el consentimiento del titular en el caso mencionado.

Agregó que debía incorporarse a este artículo una letra f) adicional, del siguiente tenor:

“f) Cuando el tratamiento de los datos sea necesario para la formulación, ejercicio o defensa de un derecho ante los tribunales de justicia.”.

El asesor del Comité Udi, señor Mery señaló no estar de acuerdo con esta idea. Agregó que no es necesario reiterarlo en este caso concreto.

Respecto a la acotación realizada por el Presidente de la Comisión, Honorable Senador señor Harboe, en relación a la ley N° 20.584, constató que efectivamente el artículo en estudio debe estar en correlación con los derechos de los pacientes. Subrayó que los propietarios de los datos son estos últimos y ninguna redacción se puede entender como una derogación tácita de lo dispuesto en otros cuerpos legales.

Seguidamente, propuso reemplazar en el inciso final el término “puede”, por “pueden”, porque se refiere a los resultados de los estudios.

Puesto en votación el artículo 16 bis, con las enmiendas indicadas, fue aprobado por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores De Urresti, Harboe y Moreira.

En una sesión posterior, los representantes del Ejecutivo propusieron agregar una letra g) nueva a este precepto. En ella se dispone lo siguiente:

“g) Cuando la finalidad del tratamiento quede expresamente establecida en la ley.”.

El asesor del Ministerio de Hacienda, señor Godoy adujo que las grandes fuentes de legitimidad y de licitud del tratamiento de datos, están constituidos por el consentimiento y por la ley. Sin embargo, respecto a los datos de salud existe una exigencia mayor, a saber, que la finalidad del tratamiento quede expresamente establecida en la ley.

El Honorable Senador señor Larraín constató que se podrá hacer tratamiento de datos sensibles cuando la finalidad del mismo esté expresamente autorizada por la ley.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó la enmienda propuesta por el Ejecutivo.

Artículo 16 ter

A continuación, la Comisión se abocó al estudio del artículo 16 ter contenido en el proyecto de ley del Ejecutivo, disposición que regula los datos personales biométricos.

Este precepto establece lo siguiente:

“Artículo 16 ter.- Datos personales biométricos. El responsable que trate datos personales biométricos, tales como la huella digital, el iris, los rasgos de la mano o faciales y la voz, deberá proporcionar al titular la siguiente información específica:

a) La identificación del sistema biométrico usado.

b) La finalidad específica para la cual los datos recolectados por el sistema biométrico serán utilizados.

c) El período durante el cual los datos biométricos serán utilizados.

d) La forma en que el titular puede ejercer sus derechos.

Un reglamento regulará la forma y los procedimientos que se deben utilizar para la implementación de los sistemas biométricos.

Con todo, no se podrán crear o mantener bancos de huellas digitales o de otros datos biométricos, salvo expresa autorización legal.”.

Al iniciarse el estudio de este precepto, el grupo de asesores parlamentarios propuso a la Comisión aprobar el texto del proyecto del Ejecutivo, eliminando su inciso final.

Seguidamente, **la asesora del Ministerio de Economía, señora Bernardita Piedrabuena,** comentó que en el caso de los datos biométricos, éstos se rigen por las reglas generales del tratamiento de los datos sensibles, es decir, las consagradas en el artículo 16. Por lo tanto, cumpliendo los requisitos allí establecidos, pueden tratarse datos biométricos, siempre y cuando el titular se le proporcione la información detallada en el artículo en estudio, al momento de entregar los datos.

El Presidente de la Comisión, Honorable Senador señor Harboe manifestó que surge, nuevamente, la discusión sobre el consentimiento previo. Constató que actualmente existe un sistema que permite, a través, del reconocimiento facial, almacenar información. Advirtió que en esta hipótesis el titular debe prestar su consentimiento. Destacó que muchas veces este último ignora que la información es almacenada.

Recomendó observar la normativa norteamericana sobre la materia.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena sostuvo que el responsable que trate los datos biométricos tiene la obligación de proporcionar al titular la información que se detalla en el artículo.

El asesor del Ministerio de Hacienda, señor Godoy, expresó que en el ámbito de los datos biométricos, cuando la fuente de licitud sea el consentimiento, éste se debiera prestar previamente.

Añadió que carece de sentido que al titular le enrolen sus datos biométricos, sin haberle comunicado la finalidad del tratamiento.

El asesor del Comité Udi, señor Mery preguntó si la información que debe entregar el responsable al titular se otorga solo en una oportunidad.

El asesor del Ministerio de Hacienda, señor Godoy, manifestó que ello será regulado por el Reglamento correspondiente.

El Presidente de la Comisión, Honorable Senador señor Harboe, expuso que el desarrollo tecnológico actual es tan variable, que recomendó que el registro se lleve a cabo cada vez que un sujeto se vea enfrentado a un posible tratamiento de datos biométricos.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena, precisó que en la letra c), se establece que deberá informarse al titular, el período durante el cual los datos biométricos serán utilizados.

El Presidente de la Comisión, Honorable Senador, señor Harboe aseveró que debe regularse por ley, las responsabilidades de las empresas que efectúen el control biométrico y la utilización que hagan de los datos obtenidos.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena, relató que en la letra b), se exige que el responsable informe al titular sobre la finalidad específica para la cual los datos recolectados por el sistema biométrico serán utilizados.

La Comisión solicitó a los representantes del Ejecutivo volver a estudiar esta disposición.

En una sesión posterior, el Ejecutivo insistió en mantener la redacción de este precepto en los términos consignados precedentemente.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena señaló que respecto a los datos biométricos, es partidaria del consentimiento inequívoco, porque el consentimiento expreso debe constar por escrito, y ello dificulta su aplicación, por ejemplo, en los datos biométricos que se pueden recopilar en el transporte público o en estadios.

El Presidente de la Comisión, Honorable Senador señor Harboe advirtió que en la actualidad, el dato biométrico es cada día más masivo. Sugirió que se debe establecer una regulación que circunscribiera el uso de la información obtenida, exclusivamente para los fines de seguridad o interés público.

Asimismo, consultó por qué no se establece una limitación respecto a este tipo de datos. Propuso que se puedan obtener para fines de seguridad.

El asesor del Ministerio de Hacienda, señor Godoy manifestó que la norma propuesta en el artículo 16 ter es estricta en

relación a los datos biométricos. Constató que se pasó de un sistema de total libertad a uno regulado.

Sostuvo que si se exige consentimiento previo, la limitación viene dada por los datos recogidos con anterioridad.

Expuso que entendiendo que estamos ante un dato sensible, y que su utilización solo se puede hacer con consentimiento expreso, estarían suficientemente cautelados los derechos de los titulares de datos.

El Presidente de la Comisión, Honorable Senador señor Harboe, inquirió cuál sería la fuente de licitud de la base de datos que se está creando, qué derechos tendrá el titular de los datos biométricos recolectados.

Reiteró que debe circunscribirse la finalidad de la recolección de los mencionados datos, a una finalidad de seguridad.

El asesor del Ministerio de Hacienda, señor Godoy, sostuvo que la norma en estudio no está autorizando sistemas de televigilancia, sino que solo está regulando el sistema de tratamiento de datos biométricos.

El Presidente de la Comisión, Honorable Senador señor Harboe, afirmó que el dato biométrico de la identificación facial solo se hace a través del sistema de televigilancia.

Preguntó cómo regular los sistemas antes descritos en los lugares de acceso público.

El asesor del Ministerio de Hacienda, señor Godoy, consignó que aquellos datos biométricos que permitan identificar a una persona, están sujetos al estándar normativo regulado en el artículo en estudio.

El asesor del Honorable Senador Larraín, señor Olmedo, recalcó que en el último inciso de la disposición se hace referencia a un reglamento. Sugirió que se debe identificar el Ministerio que lo expida y expresar que la Agencia elaborará previamente un informe, cuando corresponda.

El Presidente de la Comisión puso en votación el siguiente texto:

“Artículo 16 ter.- Datos personales biométricos. El responsable que trate datos personales biométricos, tales como la huella

digital, el iris, los rasgos de la mano o faciales y la voz, deberá proporcionar al titular la siguiente información específica:

a) La identificación del sistema biométrico usado;

b) La finalidad específica para la cual los datos recolectados por el sistema biométrico serán utilizados;

c) El período durante el cual los datos biométricos serán utilizados, y

d) La forma en que el titular puede ejercer sus derechos.

Un reglamento expedido por el Ministerio de Hacienda, previo informe de la Agencia de Protección de Datos personales, regulará la forma y los procedimientos que se deben utilizar para la implementación de los sistemas biométricos.”.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó esta disposición.

Artículo 16 quater

Seguidamente, la Comisión analizó el artículo 16 quater del proyecto de ley del Ejecutivo, disposición que regula los datos personales relativos al perfil biológico humano. El texto de esta norma es el siguiente:

“Artículo 16 quater.- Datos personales relativos al perfil biológico humano. El responsable de datos sólo puede realizar tratamiento de datos personales relativos al perfil biológico del titular, tales como los datos genéticos, proteómicos o metabólicos, para los siguientes fines:

a) Realizar diagnósticos médicos.

b) Prestar asistencia médica o sanitaria en caso de urgencia.

c) Realizar estudios o investigaciones científicas, médicas, epidemiológicas, antropológicas, arqueológicas o de medicina forense, que vayan en beneficio de la salud humana.

d) Cumplir resoluciones judiciales recaídas en procesos civiles, de familia o penales.

Queda prohibido el tratamiento y la cesión de los datos relativos al perfil biológico de un titular y las muestras biológicas asociadas a una persona identificada o identificable, incluido el almacenamiento del material biológico, cuando los datos o muestras han sido recolectados en el ámbito laboral, educativo, deportivo, social o de seguros, salvo que la ley expresamente autorice su tratamiento en casos calificados.

Los prestadores institucionales de salud, sean públicos o privados, que requieren tratar datos personales relativos al perfil biológico humano dentro del marco de las funciones que les señala el Código Sanitario o la ley Nº 20.120 y su normativa complementaria, deben adoptar y mantener los más altos estándares de control, seguridad y resguardo de esta información y de las muestras biológicas recolectadas.

El resultado de los estudios e investigaciones científicas que utilicen datos personales relativos al perfil biológico humano pueden ser publicados o difundidos libremente, debiendo previamente anonimizarse los datos que se publiquen.”.

Al iniciarse el estudio de esta proposición, el grupo de asesores parlamentarios sugirió a la Comisión aprobar el proyecto de ley del Ejecutivo, agregando, en el inciso primero, la frase “Cumpliéndose lo dispuesto en el artículo 16”.

Asimismo, **la asesora del Ministerio de Economía, señora Piedrabuena,** explicó que en el inciso final de este precepto, cuando habla de anonimizar los datos que se publiquen, se refiere a que aquello debe suceder en la publicación de los datos y no en la base de datos.

El asesor del Comité Udi, señor Mery, sugirió reemplazar en el inciso final, la expresión “pueden”, por “puede”, ya que con ella se está refiriendo al resultado de los estudios e investigaciones científicas.

El Presidente de la Comisión, Honorable Senador señor Harboe precisó que el artículo dice relación con la necesidad de resguardar los datos genéticos de una persona, que se somete a un tratamiento de salud.

Finalmente, consultó si la redacción propuesta por el Ejecutivo tomó en consideración la normativa europea.

El asesor del Ministerio de Hacienda, señor Godoy, expresó que la redacción tiene su fuente en la normativa europea, pero se tuvo a la vista el estándar OCDE. Agregó que se está innovando en esta materia.

El Presidente de la Comisión, Honorable Senador señor Harboe, preguntó si era taxativa la enumeración del inciso segundo, cuando se prohíbe el tratamiento y la cesión de los datos relativos al perfil biológico de un titular y las muestras biológicas asociadas a una persona identificada o identificable, incluido el almacenamiento del material biológico, cuando los datos o muestras han sido recolectados en el ámbito laboral, educativo, deportivo, social o de seguros.

Inquirió si puede exigírsele datos genéticos, protéomicos o metabólicos a un ciudadano que ingresa a un edificio

La asesora del Ministerio de Economía, señora Piedrabuena, reconoció que dicha hipótesis no fue considerada.

El asesor del Ministerio de Hacienda, señor Godoy, propuso ampliar la prohibición impuesta por el inciso segundo, al ámbito de la seguridad o identificación.

El Honorable Senador señor De Urresti hizo mención a la parte final del inciso segundo, que señala lo siguiente: “salvo que la ley expresamente autorice su tratamiento en casos calificados”. En relación a esta disposición, preguntó a qué casos se refiere.

El asesor del Ministerio de Hacienda, señor Godoy, respondió que un caso en que se aplicaría esta norma sería, por ejemplo, en aquel en que la ley autorice a los bancos de información genética que utilicen la mencionada información para determinar la filiación de una persona. Hizo presente que lo relevante es que cuando se tomen muestras de material biológico, éstas tengan una finalidad específica, prescrita por la ley. Añadió que se podrán utilizar para un fin distinto, solo con autorización legal expresa.

Puesto en votación el artículo 16 quater, con la enmienda de agregar en el inciso segundo, a continuación del término “de seguros” la frase “de seguridad o identificación”, fue aprobado por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores De Urresti, Harboe y Larraín.

En una sesión posterior, los representantes del Ejecutivo, señora Piedrabuena y señor Godoy, propusieron reemplazar las letras c) y d) de la norma aprobada por las siguientes:

“c) Efectuar estudios o investigaciones científicas, médicas o epidemiológicas que vayan en beneficio de la salud humana o investigaciones antropológicas, arqueológicas o de medicina forense.

d) Ejercer un derecho ante los tribunales de justicia.

e) Los expresamente establecidos en la ley”.

El Presidente de la Comisión, Honorable Senador señor Harboe consultó por qué se modificó la letra d).

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena sostuvo que se quiso homologar las hipótesis de los casos en que está permitido el uso de los datos de salud con los datos de perfil biológico.

El Presidente de la Comisión, Honorable Senador señor Harboe preguntó si el cambio de criterio puede generar una disminución del ámbito de aplicación de esta disposición.

Agregó que se puede dar el caso de que una persona sea notificada de una determinada condena. En esa hipótesis no estará ejerciendo un derecho.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena sugirió la siguiente redacción para la letra d):

“d) Ejercer un derecho ante los tribunales o cumplir resoluciones judiciales.”.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó estas nuevas letras propuestas por el Ejecutivo.

Artículo 16 quinquies

A continuación, la Comisión trató el artículo 16 quinquies del proyecto de ley del Ejecutivo, disposición que regula los datos personales relativos a los niños, niñas y adolescentes.

En este precepto se señala que el tratamiento de los datos personales que conciernen a los niños, niñas y adolescentes solo se puede realizar atendiendo al interés superior de éstos y al respeto de su autonomía progresiva.

Agrega que cumpliéndose la exigencia establecida en el inciso anterior, es necesario contar con el consentimiento otorgado en forma específica, expresa y previa por quien tiene a su cargo el cuidado personal de los niños y adolescentes, salvo que expresamente lo autorice o mandate la ley.

Añade que los datos personales de los adolescentes, salvo los datos personales sensibles, se pueden tratar de acuerdo a las normas de autorización previstas en esta ley para los adultos. Los datos personales sensibles de los adolescentes sólo se podrán tratar con el consentimiento otorgado en forma específica, expresa y previa por quien tiene a su cargo el cuidado personal, salvo que expresamente lo autorice o mandate la ley.

Precisa que para los efectos de esta ley se consideran niños a los menores de catorce años, y adolescentes a los mayores de catorce y menores de dieciocho años.

Es una obligación especial de los establecimientos educacionales y de todas las personas o entidades públicas o privadas que traten o administren datos personales de niños, niñas y adolescentes, incluido quienes ejercen su cuidado personal, velar por el uso lícito y la protección de la información personal que concierne a los niños, niñas y adolescentes.”.

En el análisis de este precepto, la Comisión tuvo a la vista el artículo 10 de la Moción parlamentaria que se refunde en este informe. Su texto es el siguiente:

“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.”.

Al iniciarse el estudio de esta materia, el grupo de asesores parlamentarios sugirió a la Comisión aprobar el proyecto del Ejecutivo, enmendado en el siguiente sentido:

Artículo 16 quinquies.- Datos personales relativos a los niños, niñas y adolescentes. El tratamiento de los datos personales que conciernen a los niños, niñas y adolescentes, sólo puede realizarse atendiendo al interés superior de éstos y al respeto de su autonomía progresiva.

Cumpliéndose la exigencia establecida en el inciso anterior, para tratar los datos personales de los niños y niñas se requiere el consentimiento otorgado por quien tiene a su cargo el cuidado personal del niño o niña, salvo que expresamente lo autorice o mandate la ley.

Los datos personales de los adolescentes se podrán tratar de acuerdo a las normas de autorización previstas en esta ley para los adultos, salvo lo dispuesto en el inciso siguiente.

Los datos personales sensibles de los adolescentes menores de 16 años, sólo se podrán tratar con el consentimiento otorgado por quien tiene a su cargo el cuidado personal del menor, salvo que expresamente lo autorice o mandate la ley.

Para los efectos de esta ley, se consideran niños o niñas a los menores de catorce años, y adolescentes, a los mayores de catorce y menores de dieciocho años.

Constituye una obligación especial de los establecimientos educacionales y de todas las personas o entidades públicas o privadas que traten o administren datos personales de niños, niñas y adolescentes, incluido quienes ejercen su cuidado personal, velar por el uso lícito y la protección de la información personal que concierne a los niños, niñas y adolescentes.”.

Sobre estos preceptos, el señor Presidente de la Comisión otorgó el uso de la palabra **al asesor del Ministerio de Hacienda, señor Godoy,** quien hizo presente que el contenido de esta disposición fue uno de los más debatidos al interior del grupo de asesores parlamentarios, que revisó y trató de integrar las propuestas del Ejecutivo y de la Moción parlamentaria.

Luego, aclaró que la regulación que se propone responde a la opinión mayoritaria de la mencionada instancia.

Precisó que se establece una regla que consiste en que para el tratamiento de los datos de los menores de 14 años, se exige la autorización de sus padres. Explicó que se instaura una regla intermedia para el caso de los datos sensibles.

Agregó que durante el estudio de esta materia, el asesor del Honorable Senador, señor Espina, señor Pablo Urquízar, propuso establecer, como requisito uniforme de edad, los 18 años, sin hacer distinción entre datos sensibles y no sensibles.

Seguidamente, aclaró que en general la legislación hace una distinción entre adolescentes y niños, y promueve que existan reglas más estrictas respecto al tratamiento de los datos de los niños.

El asesor del Comité Udi, señor Mery expresó que en el primer inciso del artículo en estudio, se utiliza la expresión: “al respeto de su autonomía progresiva”. Propuso como redacción alternativa, la siguiente: “tomar en consideración siempre su opinión, edad y grado de madurez.”.

Asimismo, indicó que en el inciso segundo se señala: “quien tiene a su cargo el cuidado personal del niño o niña”. Sugirió reemplazarlo por: “padres, representantes legales o quienes tienen el cuidado personal del niño o niña”.

El asesor del Ministerio de Hacienda, señor Godoy, recordó a la Comisión que la legislación en materia de infancia avanza hacia el concepto de la autonomía progresiva. Agregó que la redacción propuesta se orienta en esa dirección.

Destacó que resulta relevante recoger los principios de la Convención de los Derechos del Niño, que ya forma parte de nuestro ordenamiento jurídico.

Asimismo, se mostró de acuerdo con la modificación sugerida de nombrar en primer lugar a los padres, antes de quien tenga a su cargo el cuidado personal.

Constató que, en relación a la edad, toda la legislación moderna en esta materia reconoce crecientes niveles de autonomía respecto de los adolescentes y jóvenes.

El Presidente de la Comisión, Honorable Senador señor Harboe, recordó que el concepto de la autonomía progresiva ha sido aprobado por esta Comisión en, a lo menos, dos textos legales, a saber, en el proyecto de ley que regula la despenalización de la interrupción voluntaria del embarazo por tres causales y en la iniciativa que regula entrevistas grabadas en video y, otras medidas de resguardo a menores de edad, víctimas de delitos sexuales.

Puesto en votación el artículo 16 quinquies, con la enmienda propuesta al inciso segundo, fue aprobado por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores De Urresti, Harboe y Larraín.

En seguida se sometió a votación la idea de fijar en 18 años la edad, para que se puedan tratar datos sensibles sin

contar con el consentimiento de quien tiene a su cargo el cuidado personal del menor. Esta indicación fue rechazada con los votos en contra de los Honorables Senadores señores De Urresti y Harboe. Votó a favor de esta enmienda el Honorable Senador señor Larraín.

Artículo 16 sexies

A continuación, la Comisión trató el artículo 16 sexies del proyecto de ley del Ejecutivo, disposición que se refiere a los datos personales con fines históricos, estadísticos, científicos y de estudios o investigaciones. Su texto es el siguiente:

"Artículo 16 sexies.- Datos personales con fines históricos, estadísticos, científicos y de estudios o investigaciones. Las personas naturales o jurídicas, de derecho público o privado, podrán tratar datos personales con fines históricos, estadísticos, científicos y para estudios o investigaciones que atiendan fines de interés público, cuando el titular haya prestado su consentimiento en forma inequívoca, específica, previa e informada.

El responsable de datos debe acreditar, cuando le sea requerido, que ha adoptado todas las medidas de calidad y seguridad necesarias con el objeto de resguardar que los datos se utilicen exclusivamente para tales fines. Cumplidas estas condiciones, el responsable puede almacenar y utilizar los datos por un período indeterminado de tiempo.

Los registros o bases de datos que se traten con estos fines se pueden ceder a otras personas naturales o jurídicas, previo consentimiento del titular y siempre que los cesionarios los utilicen para los mismos fines. El cedente debe asegurarse que el cesionario adopte medidas de calidad y seguridad iguales o superiores a las adoptadas por él.

Los responsables que hayan tratado datos personales exclusivamente con estas finalidades pueden efectuar publicaciones con los resultados y análisis obtenidos, debiendo previamente adoptar las medidas necesarias para anonimizar los datos que se publiquen.

En relación a este precepto el grupo de asesores parlamentarios sugirió a la Comisión aprobar este precepto con las siguientes enmiendas:

"Artículo 16 sexies.- Datos personales con fines históricos, estadísticos, científicos y de estudios o investigaciones. **Se entiende que existe un interés legítimo en el tratamiento de datos personales que realicen las personas naturales o jurídicas, públicas o**

privadas, incluidos los organismos públicos, cuando el tratamiento se realiza exclusivamente con fines históricos, estadísticos, científicos y para estudios o investigaciones que atiendan fines de interés público.

Los responsables de datos deberán adoptar y acreditar que ha cumplido con todas las medidas de calidad y seguridad necesarias para resguardar que los datos se utilicen exclusivamente para tales fines. Cumplidas estas condiciones, el responsable podrá almacenar y utilizar los datos por un período indeterminado de tiempo.

Los responsables que hayan tratado datos personales exclusivamente con estas finalidades podrán efectuar publicaciones con los resultados y análisis obtenidos, debiendo previamente adoptar las medidas necesarias para anonimizar los datos que se publiquen.”.

Sobre esta proposición, **la asesora del Ministerio de Economía, señora Piedrabuena,** destacó que hay datos personales que son muy valiosos para investigaciones científicas o estudios de políticas públicas. Afirmó que lo que se pretende con esta norma es otorgar una fuente de legitimidad al uso de datos personales para efectos de estudio. Agregó que la norma también contempla obligaciones que en esta materia debe cumplir el responsable de datos.

El asesor del Comité Udi, señor Mery, consultó si sería contrario a las reglas establecidas en esta ley la publicación de datos de personas que aparecen mencionadas en las revistas de jurisprudencia.

La asesora del Ministerio de Economía, señora Piedrabuena precisó que no sería contrario a la ley si se fundamenta un interés legítimo.

Concluido el análisis de esta disposición, el señor Presidente de la Comisión, la sometió a votación.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores De Urresti, Harboe y Larraín, aprobó el proyecto de ley del Ejecutivo, con las enmiendas sugeridas por el grupo de asesores.

Artículo 16 septies

En seguida, la Comisión consideró el artículo 16 septies del proyecto de ley del Ejecutivo, disposición que regula el uso de

datos personales que se recopilan por geolocalización o movilidad. El texto de este precepto es el siguiente:

"Artículo 16 septies.- Datos de geolocalización. El tratamiento de los datos personales de geolocalización o de movilidad del titular se puede efectuar cuando el titular haya prestado su consentimiento en forma inequívoca.

El titular de datos deberá ser informado de manera clara, suficiente y oportuna, antes de obtener su consentimiento, del tipo de datos de geolocalización o movilidad que serán tratados, de la finalidad y duración del tratamiento y si los datos se comunicarán o cederán a un tercero para la prestación de un servicio con valor añadido.

En cualquier momento el titular podrá revocar el consentimiento otorgado.

Los datos de geolocalización se podrán tratar sin limitaciones cuando previamente hayan sido anonimizados.".

Al iniciarse el estudio de esta materia, el grupo de asesores parlamentarios sugirió a la Comisión, aprobar este artículo, modificado en los siguientes términos:

"Artículo 16 septies.- Datos de geolocalización. El tratamiento de los datos personales de geolocalización o de movilidad del titular se podrá **realizar bajo las mismas bases de licitud establecidas en los artículos 12 y 13 de esta ley**.

El titular de datos deberá ser informado de manera clara, suficiente y oportuna, del tipo de datos de geolocalización o movilidad que serán tratados, de la finalidad y duración del tratamiento y si los datos se comunicarán o cederán a un tercero para la prestación de un servicio con valor añadido.".

Sobre esta disposición, **el asesor del Ministerio de Hacienda, señor Godoy,** manifestó que los mencionados datos dicen relación con el tratamiento masivo de grandes volúmenes de datos. Ratificó que en esta propuesta no se están introduciendo reglas distintas del tratamiento general de datos.

Estimó que este artículo es valioso, ya que precisa que la información de geolocalización corresponde a datos personales. Admitió que estamos ante una regla que tiene el valor de rescatar y otorgarle importancia y significación a este tipo de información.

Finalmente, planteó que quizás sería conveniente eliminar el vocablo movilidad ya que ello puede generar confusión.

En seguida, **el asesor del Comité Udi, señor Mery,** preguntó cómo se condice esta norma con aquellas que regulan el monitoreo electrónico, como el brazalete. Preguntó si este caso sería un ejemplo de las hipótesis establecidas en artículo 13 (otras fuentes de licitud del tratamiento de datos).

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena manifestó que aquello es así, que la fuente de legitimidad es la ley.

El asesor del Ministerio de Hacienda, señor Godoy, precisó que el Título IV de la ley n° 19.628, que se mantiene en la presente iniciativa, contempla una extensa regulación de los datos personales por parte de los órganos públicos, donde se consideran, por ejemplo, las actividades vinculadas con la persecución penal. Admitió que cuando se revise dicho título, se deben revisar las reglas sobre tratamiento y de control de datos que efectúan los órganos públicos.

En análisis posterior del mencionado artículo, el Ejecutivo propuso eliminar en el inciso primero la expresión “o de movilidad” y en el inciso segundo “o movilidad”.

El asesor del Ministerio de Hacienda, señor Godoy señaló que este tipo de datos son conocidos como de geolocalización. Afirmó que esta última incluye la movilidad.

El Presidente de la Comisión, Honorable Senador señor Harboe constató que actualmente existe tecnología disponible que es capaz de no solo ubicar a una persona en determinado lugar, mediante la geolocalización, sino que además, permite seguirla.

Preguntó qué sucede con la información que es capaz de captar dicha tecnología.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena expuso que si mediante la geolocalización se referencia a cada segundo, accedo a la movilidad.

El Presidente de la Comisión, Honorable Senador señor Harboe sugirió estudiar con más detalle esta disposición durante el debate en particular de este proyecto de ley.

Concluido el análisis de este precepto, la Comisión, por la unanimidad de sus miembros presentes, Honorables

Senadores señores Araya, Harboe y Larraín, aprobó el texto del proyecto de ley del Ejecutivo, con las enmiendas sugeridas por el grupo de asesores y la eliminación del término “movilidad”.

Artículo 17

En seguida la Comisión trató una modificación que el Ejecutivo propone al artículo 17 de la ley N° 19.628, disposición que inaugura el Título III de la ley y que se refiere a la utilización de datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial.

La referida norma señala un conjunto de restricciones a las que están sometidos los responsables de los registros o bancos de datos.

Sobre esta materia, el Ejecutivo propone reemplazar la expresión “banco de datos” por “base de datos”, las tres veces que aparece en su texto.

Al explicar este cambio, **la asesora del Ministerio de Economía, señora Bernardita Piedrabuena,** consignó que el mismo está en concordancia a los cambios que el proyecto hace en materia de definiciones.

Dada esta explicación, el señor Presidente de la Comisión dio por concluido el análisis de este precepto.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores De Urresti, Harboe y Larraín, aprobó sin enmiendas esta modificación.

-.-.-

En seguida, la Comisión consideró **los artículos artículos 22 y 23 de la moción parlamentaria** que se refunde en este informe.

En estos preceptos se incorpora un Título IV a la ley N° 19.628, referido al tratamiento de datos relativos a obligaciones de carácter económico, financiero, bancario o comercial.

Estas disposiciones señalan lo siguiente:

“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 N° 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.”

La Comisión, por la unanimidad de sus miembros presentes, señores Araya, Harboe y Larraín, acordó rechazar estas enmiendas. Se estimó que esta materia podía ser considerada nuevamente durante el estudio en particular de este proyecto de ley.

-.-.-.-

Artículo 19

A continuación, la Comisión trató las modificaciones que el proyecto de ley del Ejecutivo propone al artículo 19 de la ley N° 19.628.

Cabe recordar que este precepto señala que el pago o la extinción de obligaciones por cualquier otro modo, no produce la caducidad o la pérdida de fundamento legal de los datos. Asimismo, consigna que extinguida una obligación hay que comunicar este hecho al responsable del registro o banco de datos. Concluye que las infracciones a las disposiciones que establece este precepto se sancionarán de conformidad a lo prescrito en el artículo 16.

En relación a este precepto, el proyecto del Ejecutivo sugiere tres modificaciones de concordancia, que tienen por objeto adecuar esta disposición a cambios que se han aprobado precedentemente.

Dichos cambios son los siguientes:

a) Reemplázase en el inciso primero el guarismo “12” por el guarismo “4°”.

b) Reemplázase la frase “bancos de datos” por la expresión “bases de datos” todas las veces que aparece en el texto.

c) Sustitúyese en el inciso final la frase “de acuerdo a lo previsto en el artículo 16” por la frase “de conformidad a lo dispuesto en el título VII de esta ley.”.

Al iniciarse el estudio de esta enmienda, **la asesora del Ministerio de Economía, señora Piedrabuena,** manifestó que la modificación responde a un ajuste de las referencias.

El Presidente de la Comisión, Honorable Senador señor Harboe hizo presente que se está manteniendo el principio de que cuando un deudor cumpla con su obligación, no caduca el dato. Señaló que esta discusión debe darse cuando se estudie en particular este proyecto de ley.

Puestas en votación las enmiendas al artículo 19, fueron aprobadas por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores De Urresti, Harboe y Larraín.

Artículo 20

A continuación, la Comisión consideró las enmiendas que el proyecto de ley del Ejecutivo propone al Título IV de la ley N° 19.628, que está referido al tratamiento de datos por los organismos públicos.

El primer artículo de este Título es el número 20. Este precepto dispone que el tratamiento de datos personales por parte de un organismo público sólo podrá efectuarse respecto de las materias de su competencia y con sujeción a las reglas precedentes. En esas condiciones, no necesitará el consentimiento del titular.

En relación a esta disposición el proyecto de ley del Ejecutivo propone su sustitución por la siguiente:

“Artículo 20.- Regla general del tratamiento de datos por órganos públicos. Es lícito el tratamiento de los datos personales que efectúan los órganos públicos cuando se realiza para el cumplimiento de sus funciones legales, dentro del ámbito de sus competencias, de conformidad a las normas establecidas en sus leyes especiales y a las disposiciones previstas en este título. En esas condiciones, los órganos públicos actúan como responsables de datos y no requieren el consentimiento del titular para tratar sus datos personales.

Los órganos públicos tampoco requieren el consentimiento del titular cuando, cumpliendo las exigencias establecidas en el inciso anterior, realizan tratamiento de datos personales exclusivamente con fines históricos, estadísticos o científicos y para estudios o investigaciones que atiendan fines de interés público.”.

Al iniciarse el estudio de este precepto, la Comisión tuvo presente el artículo 34 contenido en la moción parlamentaria que se refunde en este informe. Esta disposición prescribe lo siguiente:

“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.”.

El Presidente de la Comisión declaró inadmisible este precepto por regular una materia que corresponde a la iniciativa exclusiva de S.E el Presidente de la República, de conformidad a lo que dispone el número 2° del artículo 65 de la Constitución Política de la República.

A continuación, la Comisión volvió a considerar el artículo 20 propuesto por el Ejecutivo.

Sobre esta materia el Ejecutivo hizo llegar a la Comisión una indicación para reemplazar el artículo 20 propuesto por el siguiente:

“Título IV
Del tratamiento de datos personales por los órganos públicos

“Artículo 20.- Regla general del tratamiento de datos por órganos públicos. Es lícito el tratamiento de los datos personales que efectúan los órganos públicos cuando se realiza para el cumplimiento de sus funciones legales, dentro del ámbito de sus competencias, de conformidad a las normas establecidas en sus leyes especiales, y a las disposiciones previstas en este Título. En esas condiciones, los órganos públicos actúan como responsables de datos y no requieren el consentimiento del titular para tratar sus datos personales.”.

Al considerarse esta nueva propuesta, **el asesor del Ministerio de Hacienda, señor Godoy,** ratificó que la enmienda que se sugiere es una de las más importantes del proyecto de ley en estudio. Ella consiste en una nueva regulación del tratamiento de datos por parte de los órganos públicos.

Agregó que uno de los mayores tratadores de datos son los entes públicos. Constató que las últimas modificaciones legales que se han efectuado a los distintos servicios públicos han creado o incorporado algunas normas referidas al tratamiento de datos personales. No obstante lo anterior, subrayó que la mayoría de los órganos de la administración del Estado, y los poderes del Estado, no tienen, dentro de sus normas orgánicas, reglas especiales para el tratamiento de datos. Por lo tanto, afirmó estamos ante las normas que, en términos generales, van a regir la actividad de tratamiento de datos por parte de los organismos públicos.

Sostuvo que las normas de esta ley se aplicarán a todos los servicios de la administración del Estado que no tengan normas especiales para el tratamiento de datos personales.

Añadió que los organismos públicos pueden tratar datos personales, siempre y cuando realicen esta labor para el cumplimiento de sus funciones legales y dentro del ámbito de sus competencias.

El asesor del Comité Udi, señor Mery, aseguró que la redacción guarda correspondencia con el artículo 6° de nuestra Carta Fundamental.

En todo caso, propuso reemplazar la frase: “de conformidad a las normas establecidas en sus leyes especiales”, por la siguiente: “de conformidad a las normas establecidas en la ley”.

Asimismo, preguntó por qué circunscribir la referencia únicamente a los estatutos especiales y al presente cuerpo legal, si pudiese haber otros preceptos legales aplicables.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena, estimó pertinente el comentario del asesor, señor Mery, y se mostró de acuerdo con modificar este precepto en los términos ya sugeridos.

El asesor del Ministerio de Hacienda, señor Godoy, precisó que cuando se menciona “leyes especiales”, no se está refiriendo esta norma, necesariamente, a las leyes orgánicas.

El Presidente de la Comisión, Honorable Senador señor Harboe, consultó si la presente iniciativa será supletoria de las leyes de cada servicio público.

El Honorable Senador señor Larraín aseveró que el presente artículo debe relacionarse con el artículo 24, porque este último establece el régimen de excepciones.

Hizo presente que dicha disposición establece lo siguiente:

Artículo 24.- Régimen de excepciones. Las disposiciones de la presente ley no se aplican a los órganos públicos que, actuando en cumplimiento de sus funciones legales y dentro del ámbito de sus competencias, realizan tratamiento de datos personales en los siguientes casos:

a) Cuando efectúen tratamiento de datos que se encuentran protegidos por normas de secreto o confidencialidad establecidas en sus respectivas leyes. Cuando en cumplimiento de una obligación legal un órgano público comunica o cede a otro órgano público datos protegidos por normas de secreto o confidencialidad, el organismo público receptor deberá tratarlos manteniendo la misma obligación de secreto o confidencialidad.

b) Cuando realicen tratamiento de datos personales para la investigación, persecución, enjuiciamiento o sanción de infracciones penales, civiles y administrativas.

c) Cuando efectúen operaciones de tratamiento de datos personales en actividades relacionadas con la seguridad de la nación, la defensa nacional o la mantención del orden público o la seguridad pública.

d) Cuando se haya declarado estado de catástrofe o estado de emergencia, de conformidad a la ley y mientras permanezca vigente la respectiva declaración.

Sin perjuicio de lo señalado en el inciso anterior, los tratamientos de datos personales que realicen los organismos públicos deberán cumplir siempre con los principios de licitud del tratamiento, calidad, seguridad y responsabilidad establecidos en esta ley.”.

Por lo mismo, inquirió si todas las excepciones están consagradas en el mencionado artículo. Constató que si así fuere, las leyes especiales no prevalecerán.

El asesor del Honorable Senador Larraín, señor Olmedo, expresó que la expresión: “leyes especiales”, resulta bastante reduccionista. Recalcó que se desconoce cuántas leyes contemplan normas de datos personales. Enfatizó que la redacción del nuevo texto propuesto por el Ejecutivo, deja abierto un estatuto desconocido, que el presente proyecto de ley debe rectificar.

El asesor del Comité del PPD, señor Sebastián Abarca, remarcó que debe analizarse la naturaleza jurídica del proyecto de ley en estudio. Destacó que el objeto de éste, consiste en regular todas las materias de protección de datos.

Aseveró que la presente iniciativa tiene la pretensión de ser un cuerpo legal general. Por consiguiente, declaró que la idea de supletoriedad tendrá que recoger los principios que contiene esta ley.

El asesor del Ministerio de Hacienda, señor Godoy, consignó que un número importante de los estatutos que rigen a los organismos públicos, no contemplan reglas para el tratamiento de datos personales. Por lo tanto, precisó, los tratamientos de datos que realicen esos organismos se regirán por las reglas generales establecidas en este proyecto de ley.

Sostuvo que existen algunas instituciones que cuentan con reglas especiales para el tratamiento de datos, tal como, la ley N°20.584 que regula los derechos y deberes que tienen las personas en relación con acciones vinculadas a su atención en salud.

Remarcó que la norma en discusión constituye el estatuto que se aplicará a los órganos de la administración del Estado que realicen tratamiento de datos.

Ratificó que la iniciativa en estudio establece que los organismos públicos pueden realizar tratamiento de datos para el cumplimiento de sus funciones, y dentro del ámbito de sus competencias.

Reconoció que puede haber una ley particular que le otorgue un mandato especial a un organismo público, pero el estatuto general a aplicar, está presente en esta iniciativa.

Se mostró de acuerdo con la propuesta del asesor, señor Mery, de reemplazar la frase: “de conformidad a las normas establecidas en sus leyes especiales”. Sugirió modificarla por la siguiente: “de conformidad a las normas establecidas en la ley y a las disposiciones previstas en este título”.

El Honorable Senador señor Larraín expresó que pueden haber distintas leyes, no necesariamente especiales, que regulen las competencias que pueda tener un determinado organismo.

Se mostró partidario de aprobar el artículo con la enmienda propuesta.

El Presidente de la Comisión, Honorable Senador señor Harboe mostró su preocupación respecto de la vigencia de estas normas. Señaló que esta ley fijará un estándar en materia de protección de datos que será cumplido solo por los particulares, porque en el caso de los organismos públicos, podrán existir estándares distintos, en virtud de lo que disponen o podrán disponer en el futuro leyes especiales.

La asesora del Ministerio de Economía, señora Piedrabuena, recordó que el artículo 20 dispone que los órganos públicos deben someterse a las disposiciones previstas en este Título.

El Honorable Senador señor Larraín manifestó que es relevante la parte final del artículo mencionado, cuando señala: “En esas condiciones, los órganos públicos actúan como responsables de datos y no requieren el consentimiento del titular para tratar sus datos personales.”.

Agregó que en el artículo siguiente se consagran los principios y normas aplicables al tratamiento de datos de los órganos públicos.

Asimismo, consignó que la prescindencia del consentimiento del titular puede constituir una autorización muy amplia para el tratamiento de los datos.

El asesor del Ministerio de Hacienda, señor Godoy, puntualizó que deben cumplirse ciertas condiciones para que no se requiera el consentimiento del titular.

La asesora del Ministerio de Economía, señora Piedrabuena insistió que el órgano público solo puede tratar los datos personales en el ámbito de sus funciones legales, dentro de su competencia y de conformidad a las disposiciones establecidas en el Título IV de esta ley.

El asesor del Honorable Senador Larraín, señor Olmedo, hizo presente que el texto que se somete a discusión, configura un estatuto especial para el sector público en materia de protección de derecho de los ciudadanos.

El Presidente de la Comisión, Honorable Senador señor Harboe expresó que dada la particularidad del Sector Público, parece atendible generar un estatuto especial respecto al mundo privado. En todo caso, indicó que en este ámbito no hay que establecer normas menos exigentes en materias de protección de datos.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena aseveró que no se está dejando al Sector Público en una situación especial con respecto a los privados.

Precisó que no se quiere plantear, bajo ninguna circunstancia, que los órganos públicos podrán tener estándares y obligaciones diferentes y más bajos que la de los privados.

Manifestó que la excepción la constituye la fuente de legitimidad y en ciertos casos, cómo se ejercen los derechos de los titulares.

Puesto en votación el artículo 20, con las enmiendas propuestas, fue aprobada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores De Urresti, Harboe y Larraín.

Artículo 21

A continuación, la Comisión se dedicó al estudio de los principios y normas aplicables al tratamiento de datos de los órganos públicos.

El proyecto de ley del Ejecutivo regula esta materia en el artículo 21 que sustituye al actual artículo 21 de la ley N° 19.628.

La norma vigente establece que 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.

Agrega que se exceptúa de esta disposición 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.

La norma contenida en el proyecto de ley del Ejecutivo regula los principios y normas aplicables al tratamiento de datos de los órganos públicos.

En este sentido, dispone que el tratamiento de los datos personales que realicen los órganos públicos se rige por los principios establecidos en el artículo 3° de esta ley y los principios de coordinación, eficiencia, transparencia y publicidad.

En virtud del principio de coordinación, los organismos públicos deben propender a un alto grado de interoperabilidad y coherencia, de modo de evitar contradicciones en la información almacenada y reiteración de requerimientos de información o documentos a los titulares de datos. Conforme al principio de eficiencia, se debe evitar la duplicación de procedimientos y trámites entre los organismos del Estado, entre los organismos públicos y los particulares, y en los trámites y gestiones que realicen los titulares de la información. De acuerdo con los principios de transparencia y publicidad, los organismos públicos deben dar acceso a la información que tengan a su disposición, resguardando los derechos de las personas que pudieran verse afectadas por ello**, de conformidad con lo establecido en el artículo 20 de la Ley de Trasparencia de la función pública y de acceso a la información de la Administración del Estado, contenida en el artículo primero de la ley N° 20.285.**

Agrega que sin perjuicio de las demás normas establecidas en el presente título, son aplicables al tratamiento de datos que efectúen los órganos públicos las disposiciones establecidas en los artículos 14, 14 bis, 14 ter, 14 quater y 14 quinquies, los artículos de los párrafos segundo y tercero del título II, los artículos del título V y los artículos del párrafo cuarto del título VII de esta ley.

En relación con esta norma, el grupo de asesores parlamentarios sugirió a la Comisión aprobar el texto del proyecto de ley del Ejecutivo, enmendado en los siguientes términos:

“Artículo 21.- Principios y normas aplicables al tratamiento de datos de los órganos públicos. El tratamiento de los datos personales que realicen los órganos públicos se rige por los principios establecidos en el artículo 3° de esta ley y los principios de coordinación, eficiencia, transparencia y publicidad.

En virtud del principio de coordinación, los organismos públicos deben alcanzar un alto grado de interoperabilidad y coherencia, de modo de evitar contradicciones en la información almacenada y reiteración de requerimientos de información o documentos a los titulares de datos. Conforme al principio de eficiencia, se debe evitar la duplicación de procedimientos y trámites entre los organismos públicos, y entre éstos y los titulares de la información. De acuerdo con los principios de transparencia y publicidad, los organismos públicos deben dar acceso a la información que tengan a su disposición, resguardando los derechos de las personas que pudieran verse afectadas por ello.

Sin perjuicio de las demás normas establecidas en el presente Título, son aplicables al tratamiento de datos que efectúen los órganos públicos, las disposiciones establecidas en los artículos **2°**, 14, 14 bis, 14 ter, 14 quater, 14 quinquies y **15 bis**, los artículos del Párrafo Segundo y Tercero del Título II, los artículos del Título V y los artículos del Título VII de esta ley.”.

Al iniciarse el estudio de esta disposición**, la asesora del Ministerio de Economía, señora Bernardita Piedrabuena** expresó que en ella se explica cuáles son los artículos o títulos que se aplicarán al sector público.

El asesor del Honorable Senador Larraín, señor Olmedo indicó que en esta disposición no se configuran los mecanismos de control. Agregó que la mayoría de las competencias de fiscalización y de control de la Agencia están dadas respecto del sector privado.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena sostuvo que en la letra c) del artículo 31 se señala, dentro de las funciones de la Agencia:

“c) Fiscalizar el cumplimiento de las disposiciones de esta ley respecto de las operaciones y actividades de tratamiento de datos personales.”.

Apuntó que dicha letra se aplica tanto al sector privado como al público.

El asesor del Comité Udi, señor Mery, hizo presente que el inciso primero del artículo 21 hace referencia a los órganos;

en el segundo, a los organismos. Acotó que ambas nociones comprenden lo que se denomina servicio público, consagrada en el artículo 28 de la ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado. Por lo tanto, no habría modo de entender que los servicios públicos estén exentos de los preceptos de la presente ley.

Asimismo, **el Presidente de la Comisión, Honorable Senador señor Harboe,** dejó constancia que en el inciso segundo del artículo en estudio, que consagra el principio de coordinación, resulta concordante con el mismo principio consagrado en el artículo 5° de la ley N° 18.575.

El asesor del Ministerio de Hacienda, señor Godoy aseveró que el artículo 2° de la ley N° 19.628 define a los organismos públicos. Recalcó que dentro de ellos están considerados 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 1º de la ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado. Agregó que solo están excluidos aquellos organismos que tienen autonomía constitucional. Estos últimos tienen una regulación específica.

Concluido el estudio de este precepto, el señor Presidente de la Comisión lo sometió a votación.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores De Urresti, Harboe y Larraín, aprobó el artículo 21 contenido en el proyecto de ley del Ejecutivo, enmendado en la forma en que sugirió el grupo de asesores parlamentarios.

En una sesión posterior, los representantes del Ejecutivo propusieron la siguiente modificación al artículo 21:

“En el inciso segundo, para agregar luego de la palabra “resguardando” la siguiente frase: “las funciones fiscalizadoras e inspectivas y”.”.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena remarcó que debe hacerse la distinción entre ambas funciones en el tratamiento de los datos personales.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín aprobó esta proposición con una enmienda de forma.

Artículo 22

Seguidamente, la Comisión estudió la enmienda al artículo 22 de la ley 19.628, disposición que prescribe que el Servicio de Registro Civil e Identificación llevará un registro de los bancos de datos personales a cargo de organismos públicos.

Este registro tendrá carácter público y en él constará, respecto de cada uno de esos bancos de datos, el fundamento jurídico de su existencia, su finalidad, tipos de datos almacenados y descripción del universo de personas que comprende, todo lo cual será definido en un reglamento.

Agrega que el organismo público responsable del banco de datos proporcionará esos antecedentes al Servicio de Registro Civil e Identificación cuando se inicien las actividades del banco, y comunicará cualquier cambio de los elementos indicados en el inciso anterior dentro de los quince días desde que se produzca.

En reemplazo de esta disposición, el proyecto de ley del Ejecutivo contiene un nuevo artículo 22 que regula la comunicación o cesión de datos por un órgano público.

A este respecto establece que los órganos públicos están facultados para comunicar o ceder datos personales específicos o todo o parte de sus bases de datos a otros órganos públicos, siempre que la comunicación o cesión de los datos resulte necesaria para el cumplimiento de funciones legales y ambos órganos actúen dentro del ámbito de sus competencias. La comunicación o cesión de los datos se debe realizar para un tratamiento específico y el órgano público receptor no los podrá utilizar para otros fines.

Agrega que se podrán comunicar o ceder datos o bases de datos personales entre organismos públicos, cuando ellos se requieran para un tratamiento que tenga por finalidad otorgar beneficios al titular, evitar duplicidad de trámites para los ciudadanos o reiteración de requerimientos de información o documentos para los mismos titulares.

Precisa que el órgano público receptor de los datos sólo puede conservarlos por el tiempo necesario para efectuar el tratamiento específico para el cual fueron requeridos, luego de lo cual deberán ser cancelados o anonimizados. Estos datos se podrán almacenar por un tiempo mayor cuando el órgano público requiera atender reclamaciones o impugnaciones, realizar actividades de control o seguimiento, o sirvan para dar garantía de las decisiones adoptadas.

Añade, en el inciso siguiente, que para los efectos de poder comunicar o ceder datos personales a personas o entidades privadas, los organismos públicos deberán contar con el consentimiento inequívoco del titular, obtenido al momento de la recolección de los datos o con posterioridad a ella. Cuando se trate de comunicar o ceder datos personales en virtud de una solicitud de acceso a la información formulada con arreglo a lo establecido en el artículo 10 de Ley de Trasparencia de la función pública y de acceso a la información de la Administración del Estado, contenida en el artículo primero de la ley N° 20.285, los organismos públicos deberán contar con el consentimiento del titular obtenido en la oportunidad prevista en el artículo 20 de dicha ley.

Respecto de la comunicación de los datos relativos a infracciones penales, civiles, administrativas y disciplinarias, se aplicará lo dispuesto en el artículo 25 de esta ley.

Concluye que las cesiones de todo o parte de sus bases de datos personales realizadas por un órgano público deberán constar por escrito a través de un convenio suscrito por el cedente y el órgano o persona cesionaria de la información. En el convenio se establecerán las finalidades específicas de los tratamientos para los cuales se utilizarán los datos.”.

Al iniciarse el estudio de esta materia **los representantes del Ejecutivo** propusieron a la Comisión aprobar la disposición ya mencionada con algunas enmiendas, contenidas en una indicación que presentaron.

“Artículo 22.- Comunicación o cesión de datos por un órgano público. Los órganos públicos están facultados para comunicar o ceder datos personales específicos, o todo o parte de sus bases de datos o conjuntos de datos, a otros órganos públicos, siempre que la comunicación o cesión de los datos resulte necesaria para el cumplimiento de funciones legales y ambos órganos actúen dentro del ámbito de sus competencias. La comunicación o cesión de los datos se debe realizar para un tratamiento específico y el órgano público receptor no los podrá utilizar para otros fines.

Asimismo, se podrán comunicar o ceder datos o bases de datos personales entre organismos públicos, cuando ellos se requieran para un tratamiento que tenga por finalidad otorgar beneficios al titular, evitar duplicidad de trámites para los ciudadanos o reiteración de requerimientos de información o documentos para los mismos titulares.

El órgano público receptor de los datos sólo puede conservarlos por el tiempo necesario para efectuar el tratamiento específico para el cual fueron requeridos, luego de lo cual deberán ser cancelados o anonimizados. Estos datos se podrán almacenar por un tiempo mayor

cuando el órgano público requiera atender reclamaciones o impugnaciones, realizar actividades de control o seguimiento, o sirvan para dar garantía de las decisiones adoptadas.

Para los efectos de poder comunicar o ceder datos personales a personas o entidades privadas, los organismos públicos deberán contar **con el consentimiento del titular, salvo que la comunicación o cesión de datos sea necesaria para cumplir las funciones del organismo público en materia de fiscalización o inspección**.

Cuando se trate de comunicar o ceder datos personales en virtud de una solicitud de acceso a la información formulada con arreglo a lo establecido en el artículo **10 de la ley N° 20.285**, los organismos públicos deberán contar con el consentimiento del titular obtenido en la oportunidad prevista en el artículo 20 de dicha ley.

Respecto de la comunicación de los datos relativos a infracciones penales, civiles, administrativas y disciplinarias, se aplicará lo dispuesto en el artículo 25 de esta ley.

Las cesiones de todo o parte de las bases de datos realizadas por un órgano público deberán constar por escrito a través de un convenio suscrito por el cedente y el órgano o persona cesionaria de la información. En el convenio se establecerán las finalidades específicas de los tratamientos para los cuales se utilizarán los datos. La Agencia de Protección de Datos Personales en su página web pondrá a disposición de los organismos públicos modelos tipo de convenios de cesión de datos.

Los organismos públicos deberán informar mensualmente a través de su página web institucional los convenios suscritos con otros organismos públicos y con entidades privadas, sobre cesión o transferencia de datos personales.”.

En relación a esta disposición, **el asesor del Ministerio de Hacienda, señor Godoy** planteó que el artículo en discusión, viene a ratificar que, en general, las reglas que se establecen para el tratamiento de datos y para la regulación de actividades específicas del mismo, para los organismos públicos, son aún más exigentes que las que se configuran para los privados.

Apuntó que respecto de la comunicación o cesión de datos, la regulación que se propone es más estricta que la que corresponde a los privados.

Señaló que una de las debilidades que tiene el sistema de los órganos públicos consiste en que efectivamente hay

intercambios de volúmenes importantes de información entre ellos, más allá de lo estrictamente necesario. Por lo tanto, la nueva regulación establece límites estrictos sobre cómo deben ser las reglas de comunicación y de cesión de datos y por cuánto tiempo los órganos públicos que recibes esos datos, pueden mantener esa información.

Destacó que se debe procurar que las bases de datos no se cedan más allá de lo estrictamente necesario y que se produzca intercambio de información específica en cumplimiento de las funciones del órgano que la entrega y del que la recibe.

Finalmente, reiteró que en esta disposición se elevan los estándares de transparencia respecto a la información mencionada.

El asesor del Honorable Senador Larraín, señor Olmedo estimó que quedó inconclusa una fase de la transparencia que implica que esta información sea considerada en virtud del principio de transparencia activa, de la ley N° 20.285 sobre acceso a la información pública, de tal manera que la obligación de información sea fiscalizable.

El asesor del Comité Udi, señor Mery, consultó si lo propuesto en el inciso quinto no debe entenderse como una innovación sustancial al régimen vigente en la ley N° 20.285.

El asesor del Ministerio de Hacienda, señor Godoy remarcó que en el inicio de la presente discusión se señaló cuál es el marco de atribuciones de los organismos públicos para el tratamiento de datos. Consignó que lo que se está proponiendo, es que éstos, al estar cumpliendo una función establecida por ley, pueden efectuar tratamiento de datos sin necesidad de requerir el consentimiento de los titulares de datos.

Destacó que la comunicación a terceros de los datos personales de un titular requiere, por disposición de la ley, aceptación o consentimiento de dicho titular.

El Presidente de la Comisión, Honorable Senador señor Harboe sugirió que en el inciso primero, se reemplace la frase: “para el cumplimiento de funciones legales”, por: “para el cumplimiento de sus funciones legales”.

Puesto en votación el artículo 22 del proyecto de ley del Ejecutivo, enmendado en los términos reseñados precedentemente, fue aprobado por la unanimidad de los Honorables Senadores presentes, señores De Urresti, Harboe y Larraín.

En un análisis posterior, los representantes del Ejecutivo propusieron, mediante una indicación, la siguiente enmienda al artículo 22:

“Para reemplazar el inciso final por el siguiente:

“Los organismos públicos deberán informar mensualmente a través de su página web institucional los convenios suscritos con otros organismos públicos y con entidades privadas relativos a cesión o transferencia de datos personales. Esta obligación será fiscalizada por la Agencia de Protección de Datos Personales.”

El asesor del Honorable Senador Larraín, señor Olmedo acotó que el deber de información mensual debiese ser considerado como una obligación de transparencia activa y sujeta, en cuanto a la forma, a la ley N° 20.285, sobre sobre acceso a la información pública. Remarcó que en el mencionado cuerpo legal, se configura una sanción en caso de incumplimiento.

El asesor del Ministerio de Hacienda, señor Godoy indicó que con la presente iniciativa se ha tratado de separar con nitidez las competencias de la Agencia de Protección de Datos y las del Consejo para la Transparencia. Agregó que introducir la modificación sugerida por el señor Olmedo, puede provocar una confusión a la hora de fiscalizar la obligación.

Estimó que es preferible que la fiscalización la siga realizando la Agencia de Protección.

El Presidente de la Comisión, Honorable Senador señor Harboe hizo presente que no es conveniente incorporar a las dos instituciones, porque se pueden generar criterios distintos.

Añadió que lo anterior puede originar una oferta equívoca del Estado.

Puesto en votación este nuevo inciso final del artículo 22, fue aprobado por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Araya, Harboe y Larraín.

Artículo 23

A continuación, la Comisión se abocó al estudio del artículo 23 contenido en el proyecto de ley del Ejecutivo, que regula el ejercicio de los derechos del titular y reclamo de ilegalidad.

Sobre el particular dispone que el titular de datos puede ejercer ante el órgano público los derechos de acceso y rectificación que les reconoce esta ley. Agrega que no podrá cancelar ni oponerse al tratamiento de datos efectuado por un órgano público salvo que el mismo sea contrario a las disposiciones de este título.

Agrega que el ejercicio de los derechos del titular se deberá realizar de acuerdo al procedimiento establecido en el artículo 11 de esta ley, dirigiéndose al jefe superior del servicio. En todo lo no regulado se aplicarán supletoriamente las normas de la ley N° 19.880, que establece bases de los procedimientos administrativos que rigen los actos de la Administración del Estado.

Asimismo, precisa que las personas que se vean afectadas por la resolución de un órgano público, sea que les deniegue el ejercicio de un derecho reconocido en esta ley o adopte una decisión o dicte una acto que infrinja los principios y obligaciones establecidos en ella, causándole perjuicio, podrá deducir un reclamo de ilegalidad ante la Corte de Apelaciones de Santiago o del domicilio de reclamante, a su elección, de conformidad con las normas dispuestas en el artículo 47 de esta ley. El informe a que alude la letra d) del artículo 47 será evacuado por el órgano público reclamado.

Sin perjuicio de lo anterior, la Corte de Apelaciones respectiva podrá requerir informe a la Agencia de Protección de Datos Personales con el objeto de establecer si en las operaciones de tratamiento de datos realizadas por el órgano público hubo o no infracción a los principios y obligaciones establecidos en esta ley.

Al iniciarse el estudio de de este precepto **los representantes del Ejecutivo, señora Piedrabuena y señor Godoy**, sugirieron aprobar la disposición del Ejecutivo, en los siguientes términos.

“Artículo 23.- Ejercicio de los derechos del titular, procedimiento administrativo de tutela y reclamo de ilegalidad. El titular de datos podrá ejercer ante el órgano público los derechos de acceso, rectificación y oposición que le reconoce esta ley. El titular también podrá oponerse a un tratamiento específico cuando éste sea contrario a las disposiciones de este Título. El titular podrá ejercer el derecho de cancelación en los casos previstos en el inciso tercero del artículo anterior.

Con todo, no podrá solicitarse el acceso, la rectificación, la oposición, la cancelación o el bloqueo temporal de los datos personales, cuando a consecuencia de ello se impida o entorpezca el cumplimiento de las funciones fiscalizadoras o inspectivas de un organismo

público; se afecte el deber de secreto o reserva establecido en la ley, o la seguridad de la Nación.

El ejercicio de los derechos del titular se deberá realizar de acuerdo al procedimiento establecido en el artículo 11 de esta ley, dirigiéndose al jefe superior del servicio.

El titular podrá reclamar ante la Agencia de Protección de Datos Personales cuando el organismo público le haya denegado, en forma expresa o tácita, una solicitud en que ejerce cualquiera de los derechos que le reconoce esta ley. La reclamación se sujetará a las normas previstas en el procedimiento administrativo de tutela de derechos establecido en el artículo 45 de esta ley.”.

El asesor del Honorable Senador Larraín, señor Olmedo propuso que se modifique en el inciso segundo, la expresión “no podrá solicitarse el acceso”, ya que tal como está planteada implica un impedimento en el ejercicio de un derecho. Sugirió reemplazarla por: “se denegará la solicitud de acceso, de rectificación, de oposición, de cancelación o…”.

Puesto en votación el artículo 23, con la enmienda propuesta, fue aprobado por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores De Urresti, Harboe y Larraín.

En una sesión posterior, el Ejecutivo hizo llegar una indicación para reemplazar el inciso segundo de la norma aprobada por el siguiente:

“Los organismos públicos no acogerán las solicitudes de acceso, rectificación, oposición, cancelación o bloqueo temporal de los datos personales en los siguientes casos:

a) Cuando con ello se impida o entorpezca el cumplimiento de las funciones fiscalizadoras, investigativas o sancionatorias del organismo público, y

b) Cuando con ello se afecte el deber de secreto o reserva establecido en la ley.”.”

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó esta modificación.

Artículo 24

Seguidamente, la Comisión se abocó al régimen de excepciones que se aplicarán en el Sector Público.

En esta materia el proyecto de ley del Ejecutivo propone lo siguiente:

“Artículo 24.- Régimen de excepciones. Las disposiciones de la presente ley no se aplican a los órganos públicos que, actuando en cumplimiento de sus funciones legales y dentro del ámbito de sus competencias, realizan tratamiento de datos personales en los siguientes casos:

a) Cuando efectúen tratamiento de datos que se encuentran protegidos por normas de secreto o confidencialidad establecidas en sus respectivas leyes. Cuando en cumplimiento de una obligación legal un órgano público comunica o cede a otro órgano público datos protegidos por normas de secreto o confidencialidad, el organismo público receptor deberá tratarlos manteniendo la misma obligación de secreto o confidencialidad.

b) Cuando realicen tratamiento de datos personales para la investigación, persecución, enjuiciamiento o sanción de infracciones penales, civiles y administrativas.

c) Cuando efectúen operaciones de tratamiento de datos personales en actividades relacionadas con la seguridad de la nación, la defensa nacional o la mantención del orden público o la seguridad pública.

d) Cuando se haya declarado estado de catástrofe o estado de emergencia, de conformidad a la ley y mientras permanezca vigente la respectiva declaración.

Sin perjuicio de lo señalado en el inciso anterior, los tratamientos de datos personales que realicen los organismos públicos deberán cumplir siempre con los principios de licitud del tratamiento, calidad, seguridad y responsabilidad establecidos en esta ley.”.

El Presidente de la Comisión, Honorable Senador señor Harboe consultó por qué no se aplica el principio de finalidad.

El Honorable Senador señor Larraín preguntó si existe un marco de regulación de fiscalización, aparte de las leyes especiales.

El asesor del Ministerio de Hacienda, señor Godoy, consignó que en los estatutos jurídicos existen normas de excepción respecto del tratamiento de datos personales. Remarcó que el estatuto europeo reconoce dos regímenes de excepción, uno que dice relación con las normas de seguridad, y el otro con la persecución penal y la investigación de delitos.

Enfatizó que rige la legislación particular que se dicte para dichos efectos. Agregó que en el caso del enjuiciamiento penal, existe un Código que regula el proceso de investigación.

Sostuvo que respecto de la investigación civil y administrativa, todos los cuerpos legales que regulan algún procedimiento, contemplan reglas especiales del ejercicio de la acción y de la potestad del órgano. Por lo tanto, las acciones de investigación se rigen por las normas especiales que se dictan al efecto.

Precisó que las normas de la defensa nacional están excluidas.

Destacó que se innovó en incluir las situaciones de emergencia. Aseveró que en un país como el nuestro, y a partir de la experiencia del terremoto del año 2010, se realizaron diversas actividades de levantamiento de la información en terreno, que estuviera a cargo del Ministerio de Desarrollo Social.

Afirmó que los mencionados levantamientos son difíciles de llevar a cabo si no existe un mandato que permita realizar la recopilación y posterior tratamiento de los datos, sin cumplir los regímenes normales y tradicionales que un órgano público tiene que observar en situaciones de regularidad.

Sin perjuicio de lo anterior, se consideró importante incluir que, más allá de las regulaciones especiales, el tratamiento de datos que efectúen los órganos debe sujetarse a los principios de licitud, de seguridad, de calidad y responsabilidad consagrados en el cuerpo legal en estudio.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena acotó que el principio de finalidad no se introduce en el artículo en discusión, porque existen bases de datos que están en poder del Estado, y que por razones de emergencia, pueden ser utilizados con otra finalidad.

El Honorable Senador señor Larraín manifestó que los datos e informaciones presentes en las investigaciones penales tienen su propia regulación en el Código Procesal Penal. Remarcó que lo

anterior se debe complementar con la presente norma, señalando que, en esos casos no se les aplicarán las disposiciones del presente título, sin perjuicio de lo cual estarán sujetos a ciertos principios.

El Presidente de la Comisión, Honorable Senador señor Harboe detalló que en los casos de emergencia debiera crearse un estatuto jurídico especial, dentro del cual se debe autorizar a usar la información disponible para un mejor resolver.

Expresó que no excluiría el principio de finalidad tratándose de otros casos, porque se abre la puerta para que se intercambie información transgrediendo el objetivo para el cual fue recolectada o entregada.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena se mostró de acuerdo con las observaciones formuladas. En relación al principio de finalidad, indicó que éste debiese aplicarse solo en la letra a).

El Presidente de la Comisión, Honorable Senador señor Harboe hizo presente que en relación a la protección de datos, Chile es considerado un país no seguro. Agregó que dentro de las consecuencias prácticas de ello, ha significado que la Unión Europea, en reiteradas ocasiones ha negado información a Chile, respecto a determinadas personas, porque consideraban que nuestro país no daba garantías en el resguardo de la información.

Subrayó que excluir el principio de finalidad de la letra b), puede traer como consecuencia que Chile permanezca catalogado de la forma antes descrita.

Atendido lo anterior, solicitó que se revise la aplicación de finalidad.

El Honorable Senador señor Larraín solicitó no solo revisar lo del principio de finalidad, sino que también sugirió incorporar las normas propias de cada organismo y las normas generales.

En una sesión posterior, el Ejecutivo presentó una indicación para reemplazar el artículo 24 por el siguiente:

“Artículo 24.- Regímenes especiales. Las disposiciones de este Título no se aplicarán en los siguientes casos:

a) A los tratamientos de datos personales que realicen los órganos públicos competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de

ejecución de sanciones penales, incluidas las actividades de protección y prevención frente a las amenazas y riesgos contra la seguridad pública.

b) A los tratamientos de datos personales que realicen los órganos públicos competentes en materias relacionadas directamente con la seguridad de la Nación, la defensa nacional y la política exterior del país.

c) A los tratamientos de datos personales que realicen los órganos públicos competentes con el objeto exclusivo de atender una situación de emergencia o catástrofe, declarada de conformidad a la ley y sólo mientras permanezca vigente esta declaración.

Los órganos públicos y sus autoridades respectivas podrán realizar los tratamientos de datos previstos en las letras anteriores, cuando se realice para el cumplimiento de sus funciones legales, dentro del ámbito de sus competencias y de conformidad a las normas establecidas en la ley respectiva, debiendo respetar los derechos y libertades fundamentales de las personas establecidos en la Constitución Política de la República.

Con el objeto de realizar los tratamientos de datos para la finalidad prevista en la letra a) anterior, los órganos públicos y sus autoridades estarán obligadas a intercambiar información y proporcionar los datos personales que les sean requeridos para estos fines, siempre que se refieran a tratamientos que se realicen con una finalidad específica autorizada por ley o cuando esto no sea posible, el requerimiento sea una medida necesaria y proporcional.

El ejercicio de los derechos de los titulares de datos en el marco de un proceso penal, se sujetará a las normas legales específicas que regulan el proceso penal.

Los tratamientos de datos que realicen los organismos públicos en los casos previstos en este artículo deberán cumplir con los principios de licitud del tratamiento, calidad, seguridad, responsabilidad y confidencialidad establecidos en esta ley. Asimismo, los funcionarios que participen en estos tratamientos estarán sujetos a lo dispuesto en el artículo 50.”.”.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena manifestó que este artículo está dentro del Título IV, que dice relación con el tratamiento de datos personales por los órganos públicos. Agregó que artículo en discusión se refiere a los regímenes especiales.

El asesor del Ministerio de Hacienda, señor Roberto Godoy constató que la propuesta se basa en los estándares europeos. Agregó que, protegiendo los derechos de las personas, es capaz de darle facultades especiales de tratamiento de datos a aquellas autoridades e instituciones que están encargadas de tratar datos en el ámbito de la seguridad pública; la defensa nacional y durante situaciones de emergencia o catástrofe.

Seguidamente, precisó que con esta nueva redacción se busca acotar el principio de finalidad, respecto del tratamiento de datos en materia de prevención e investigación criminal. Asimismo, se persigue fijar un sistema de derechos y de protección de derechos de los titulares, en relación con los tratamientos que quedaban exceptuados en la ley.

Destacó que en la legislación comparada, el tratamiento de datos, sobre todo en materia penal, está sujeto a un estatuto jurídico particular. Recalcó que Chile carece del mencionado estatuto.

Debido a lo anterior, sostuvo que a través de esta iniciativa se deben consagrar los principios y las bases generales que van a regir el tratamiento.

Por lo tanto, argumentó, la regla que se propone consiste en que los tratamientos de datos expresados en el artículo en estudio, quedan exceptuados de las disposiciones específicas del Título que rige a los organismos públicos. Sin embargo, quedan sujetos a los principios de licitud del tratamiento; de calidad, seguridad, responsabilidad y confidencialidad.

En relación a la prevención, expresó que se establece el principio de finalidad en el intercambio de la información que se realice entre organismos públicos, y entre estos últimos y los privados. Además, se configura el deber de secreto y de reserva respecto de todos los funcionarios públicos que intervengan y participen en los tratamientos de datos.

Aseveró que recogiendo la regulación internacional en esta materia, se establece expresamente que el ejercicio de todos aquellos derechos que se ejerzan en el marco de un proceso penal se sujetará a las normas que regulan el proceso penal correspondiente.

El Presidente de la Comisión, Honorable Senador señor Harboe advirtió que también podría contemplarse una norma de reenvío que señale: “El tratamiento de datos personales sensibles se regulará por normas especiales de reserva o secreto, según

corresponda.” Afirmó que de esa forma se remite la regulación al Código Procesal Penal y a las leyes orgánicas respectivas.

El asesor del Honorable Senador Larraín, señor Olmedo, afirmó que se podría incorporar algún mecanismo que permita la defensa de derechos fundamentales frente a lo que sucede en materia de inteligencia de seguridad.

El asesor del Ministerio de Hacienda, señor Godoy aseveró que la norma en estudio es complementaria del título final de la presente ley, que regula el sistema de tratamiento de datos y el ejercicio de los derechos por parte de los titulares de los órganos autónomos constitucionales, dentro de los cuales está el Ministerio Público y los tribunales de justicia.

Constató que los titulares de datos que pudieran ver infringido o vulnerados sus derechos en esta materia, tienen los derechos que les reconoce esta ley y lo ejercerán de la forma que allí se establece.

Observó que el inciso segundo de la disposición en estudio, establece que los órganos públicos y las autoridades que realicen el tratamiento de datos lo hacen en el cumplimiento de sus funciones, dentro del ámbito de sus competencias y de conformidad a las normas establecidas en la ley respectiva. Es decir, aquellas normas que les otorgan competencia para efectos de su tratamiento.

Concluido el estudio de esta materia, el señor Presidente de la Comisión sometió a votación el nuevo artículo 24 propuesto por el Ejecutivo.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó esta disposición.

Artículo 25

A continuación, la Comisión examinó el artículo 25 del proyecto de ley del Ejecutivo que regula los datos relativos a las infracciones penales, civiles, administrativas y disciplinarias.

En este aspecto dispone que los datos personales relativos a la comisión y sanción de infracciones penales, civiles, administrativas o disciplinarias sólo pueden ser tratados por los organismos públicos para el cumplimiento de sus funciones legales, dentro del ámbito de sus competencias y en los casos expresamente previstos en la ley.

Agrega que en las comunicaciones o difusión de información que realicen los organismos públicos con ocasión del tratamiento de estos datos personales, deberán velar en todo momento porque la información comunicada o hecha pública sea exacta, suficiente, actual y completa.

Asimismo, precisa que no podrán comunicarse o hacerse públicos los datos personales relativos a la comisión y condena de infracciones penales, civiles, administrativas o disciplinarias una vez prescrita la acción penal, civil, administrativa o disciplinaria respectiva o una vez que se haya cumplido o prescrito la pena o la sanción impuesta, lo que deberá ser declarado o constatado por la autoridad pública competente. Lo anterior es sin perjuicio de la incorporación, mantenimiento y consulta de esta información en los registros que llevan los órganos públicos por expresa disposición de la ley, en la forma y por el tiempo previsto en la ley que establece la obligación específica correspondiente. Las personas que se desempeñen en los órganos públicos están obligadas a guardar secreto respecto de esta información, la que deberá ser mantenida como información reservada.

Añade que cuando la ley disponga que la información relativa a la comisión y sanción de infracciones penales, civiles, administrativas y disciplinarias deba hacerse pública a través de su incorporación en un registro de sanciones o su publicación en el sitio web de un órgano público o en cualquier otro medio de comunicación o difusión, sin fijar un período de tiempo durante el cual deba permanecer disponible esta información, se seguirán las siguientes reglas:

“a) Respecto de las infracciones penales se aplicarán los mismos plazos establecidos para la eliminación de las anotaciones prontuariales señaladas en el decreto ley N° 409, de 1932 y el decreto N° 64, de 1960, ambos del Ministerio de Justicia.

b) Respecto de las infracciones civiles, administrativas y disciplinarias permanecerán accesibles al público por el período de cinco años.

Exceptúanse de la prohibición de comunicación los casos en que la información sea solicitada por los Tribunales de Justicia u otro organismo público para el cumplimiento de sus funciones legales y dentro del ámbito de su competencia, quienes deben guardar secreto respecto de ella y mantener la debida reserva.”.

Al iniciarse el estudio de esta materia, se tuvo presente que la moción parlamentaria que se refunde en este proyecto de ley considera una normativa similar en su artículo 35. El texto de esta disposición es el siguiente:

“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.”.

Asimismo, el grupo de asesores parlamentarios sugirió a la Comisión aprobar esta disposición enmendada en los siguientes términos:

“Artículo 25.- Datos relativos a infracciones penales, civiles, administrativas y disciplinarias. Los datos personales relativos a la comisión y sanción de infracciones penales, civiles, administrativas y disciplinarias sólo pueden ser tratados por los organismos públicos para el cumplimiento de sus funciones legales, dentro del ámbito de sus competencias y en los casos expresamente previstos en la ley.

En las comunicaciones que realicen los organismos públicos, con ocasión del tratamiento de estos datos personales, deberán velar en todo momento porque la información comunicada o hecha pública sea exacta, suficiente, actual y completa.

No podrán comunicarse o hacerse públicos los datos personales relativos a la comisión y condena de infracciones penales, civiles, administrativas o disciplinarias, una vez prescrita la acción penal, civil, administrativa o disciplinaria respectiva, o una vez que se haya cumplido o prescrito la pena o la sanción impuesta, lo que deberá ser declarado o constatado por la autoridad pública competente. Lo anterior es, sin perjuicio, de la incorporación, mantenimiento y consulta de esta información en los registros que llevan los órganos públicos por expresa disposición de la ley, en la forma y por el tiempo previsto en la ley que establece la obligación específica correspondiente. Las personas que se desempeñen en los órganos públicos están obligadas a guardar secreto respecto de esta información, la que deberá ser mantenida como información reservada.

Cuando la ley disponga que la información relativa a la comisión y sanción de infracciones penales, civiles, administrativas y disciplinarias deba hacerse pública a través de su incorporación en un registro de sanciones, o su publicación en el sitio web de un órgano público o en cualquier otro medio de comunicación o difusión, sin fijar un período de

tiempo durante el cual deba permanecer disponible esta información, se seguirán las siguientes reglas:

a) Respecto de las infracciones penales, los plazos de publicidad se regirán por las normas particulares que rigen para este tipo de infracciones.

b) **Respecto de las infracciones civiles, administrativas y disciplinarias, permanecerán accesibles al público por el período de cinco años.**

Se prohíbe el tratamiento masivo de los datos personales contenidos en los registros electrónicos de infracciones penales, civiles, administrativas y disciplinarias que lleven los organismos públicos. El incumplimiento de esta prohibición constituye una infracción gravísima de conformidad a esta ley.

Exceptúense de la prohibición de comunicación los casos en que la información sea solicitada por los Tribunales de Justicia u otro organismo público para el cumplimiento de sus funciones legales y dentro del ámbito de su competencia, **quienes deberán mantener la debida reserva.**".

Sobre esta última disposición, **el asesor del Ministerio de Hacienda, señor Godoy** precisó que una norma similar existe en la ley N° 19.628. Sin embargo, el texto refundido viene a actualizarla y a fortalecerla. Añadió que se regula una situación particular que ha ido ocurriendo en distintos estatutos que es la creación de registros públicos.

El Presidente de la Comisión, Honorable Senador señor Harboe preguntó por qué se siguió un criterio distinto respecto a las infracciones civiles, administrativas, frente a las penales.

El asesor del Ministerio de Hacienda, señor Godoy respondió que en materia penal existen reglas de publicidad, en función de la gravedad del delito. Como la regla mencionada no existe en las infracciones civiles, administrativas y disciplinarias, se fijó una norma intermedia.

El Presidente de la Comisión, Honorable Senador señor Harboe adujo que las normas sobre publicidad de las infracciones penales son muy antiguas. Consideró que era el momento para actualizarlas.

El Honorable Senador señor Larraín preguntó si la redacción del inciso final permitiría que los organismos públicos busquen, dentro de sus resquicios legales, la forma de conseguir información indebida.

El asesor del Ministerio de Hacienda, señor Godoy destacó que la información está protegida por un deber de reserva. Indicó que contempla dos excepciones, a saber, el requerimiento de los tribunales y cuando un organismo público lo solicite en ejercicio de sus funciones.

Ejemplificó señalando que los organismos públicos, en la contratación de funcionarios públicos, necesitan la información respecto a las eventuales infracciones administrativas en que hubiesen incurrido. Agregó que dicha información queda registrada en la Contraloría General de la República. Enfatizó que, transcurrido cierto período de tiempo, ésta no se puede comunicar, pero podrá disponer de ella si el organismo público la llegara a necesitar, para efectos de evaluar si la persona cumple el requisito para acceder al cargo.

El Honorable Senador señor Larraín consultó si la Superintendencia de Bancos e Instituciones Financieras podrá revisar el historial comercial.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena precisó que en el artículo en estudio se habla de sanciones administrativas. Indicó que cosa distinta es si una persona tiene obligaciones económicas impagas y está en el registro de deudores. Añadió que en la ley N° 20.575, para efectos laborales, de matrículas de colegio o atenciones de emergencia, no se puede pedir, ni tratar información comercial.

Puesto en votación el artículo 25, fue aprobado por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores De Urresti, Harboe y Larraín.

Artículo 26

A continuación, la Comisión trató el artículo 26 del proyecto de ley del Ejecutivo.

Este precepto dispone lo siguiente:

“Artículo 26.- Reglamento. Las condiciones para la comunicación o cesión de datos personales entre organismos públicos y con personas u organismos privados, se regularán a través de un reglamento dictado por el Ministerio Secretaría General de la Presidencia, suscrito por el Ministro o Ministra de Hacienda. En este mismo reglamento se regularán los procedimientos de anonimización de los datos personales, especialmente los datos personales sensibles.”.

Al iniciarse su estudio, los representantes del Ejecutivo formularon una proposición aprobar este precepto en los siguientes términos:

"Artículo 26.- Reglamento. Las condiciones, **modalidades e instrumentos para** la comunicación o cesión de datos personales entre organismos públicos y con personas u organismos privados, se regularán a través de un reglamento dictado por el Ministerio Secretaría General de la Presidencia y suscrito por el Ministro o Ministra de Hacienda. En este mismo reglamento se regularán los procedimientos de anonimización de los datos personales, especialmente los datos personales sensibles."

El asesor del Ministerio de Hacienda, señor Godoy manifestó que es una norma de cierre del título, y en ella se dispone que las reglas especiales de ejecución de la ley se entregan a un reglamento, particularmente las que dicen relación con la comunicación y cesión de datos.

Agregó que desde el punto de vista de la competencia técnica, el Ministerio que tiene la coordinación de los distintos organismos públicos es el de la Secretaría General de la Presidencia.

En esta parte del debate precisó que la potestad reglamentaria pertenece al Presidente de la República y el mencionado reglamento podría ser expedido a través del Ministerio Secretaría General de la Presidencia.

El Honorable Senador señor Larraín observó que la materia en estudio quedará sujeta a órganos de gobierno. Consideró que éstas deben ser dictadas por organismos autónomos.

Remarcó que lo que se propone no cumple los estándares de independencia que establecen las reglas de la OCDE.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena precisó que la OCDE y los principios consagrados por la Red Iberoamericana de datos personales, no habla específicamente que las agencias de control tengan que ser o no parte del gobierno.

El Presidente de la Comisión, Honorable Senador señor Harboe agregó que en todo caso a este artículo se debía incorporar la frase: "y previo informe de la Agencia de Protección de Datos Personales", tal como se hace en otras disposiciones de este proyecto.

Concluido el estudio de este precepto, el señor Presidente de la Comisión lo puso en votación.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó la propuesta del Ejecutivo, con las enmiendas ya indicadas.

El texto acordado precedentemente fue ratificado mediante una indicación que presentó el Ejecutivo, la que se dio por aprobada con las votaciones señaladas precedentemente.

Artículo 27

Este precepto del proyecto de ley del Ejecutivo sustituye el artículo 23 de la ley N° 19.628, disposición que regula la indemnizaciones que la persona natural o jurídica privada o el organismo público responsable del banco de datos personales deberá cancelar por el daño patrimonial y moral que causare por el tratamiento indebido de los datos. Asimismo, precisa el procedimiento que se debe seguir en estos casos. Finalmente, determina que el monto de la indemnización será establecido prudencialmente por el juez, considerando las circunstancias del caso y la gravedad de los hechos.

El nuevo artículo 27 encabeza un nuevo título V de la ley que se refiere a la transferencia internacional de datos personales. El texto de esta disposición es el siguiente:

“Artículo 27.- Reglas aplicables a países con niveles adecuados de protección de datos. Se podrán realizar operaciones y actividades de transferencia internacional de datos personales a personas, entidades u organizaciones sujetas al ordenamiento jurídico de un país que proporcione niveles adecuados de protección de datos.

Se entiende que el ordenamiento jurídico de un país posee niveles adecuados de protección de datos, cuando cumple con estándares similares o superiores a los fijados en esta ley. La Agencia de Protección de Datos Personales determinará los países que poseen niveles adecuados de protección de datos, considerando, a los menos, lo siguiente:

a) El establecimiento de principios para el tratamiento de los datos personales.

b) La existencia de normas que reconozcan y garanticen los derechos de los titulares de datos.

c) La imposición de obligaciones de información y seguridad a los responsables del tratamiento de los datos.

d) La determinación de responsabilidades en caso de infracciones.

La transferencia internacional de datos considera las operaciones de comunicación, transmisión o cesión de datos personales, según la necesidad y finalidades del tratamiento.”.

Al iniciarse el estudio de esta materia, el grupo de asesores parlamentarios sugirió aprobar el artículo 27, en los siguientes términos:

Artículo 27.- Regla general de autorización. Son lícitas las operaciones de transferencia internacional de datos en los siguientes casos:

a) Cuando cumpliéndose los requisitos que de conformidad a esta ley confieren licitud al tratamiento de datos, la transferencia se realice a una persona, entidad u organización sujeta al ordenamiento jurídico de un país que proporcione niveles adecuados de protección de datos personales.

b) Cuando la transferencia de datos quede amparada por cláusulas contractuales u otros instrumentos jurídicos suscritos entre el responsable que efectúa la transferencia y el que la recibe y en ellas se establezcan los derechos y garantías de los titulares, las obligaciones de los responsables y los medios de control, o cuando adopten un modelo de cumplimiento o autorregulación vinculante y certificado.

c) Cuando exista consentimiento expreso del titular de datos para realizar una transferencia internacional de datos específica y determinada.

d) Cuando se refiera a transferencias bancarias, financieras o bursátiles específicas y se realicen de conformidad a su legislación aplicable.

e) Cuando la transferencia se efectúe entre sociedades o entidades que pertenezcan a un mismo grupo empresarial, empresas relacionadas o sujetas a un mismo controlador en los términos previstos en la Ley de Mercado de Valores, siempre que todas ellas operen bajo los mismos estándares y políticas en materia de tratamiento de datos personales.

f) Cuando se deban transferir datos para dar cumplimiento a obligaciones adquiridas en tratados o convenios internacionales que hayan sido ratificados por el Estado chileno y se encuentren vigentes.

g) Cuando la transferencia resulte necesaria por aplicación de convenios de cooperación, intercambio de información o supervisión que hayan sido suscritos por órganos públicos para el cumplimiento de sus funciones y en el ejercicio de sus competencias.

h) Cuando la transferencia de datos haya sido autorizada expresamente por la ley a un organismo público para el cumplimiento de sus funciones legales.

i) Cuando la transferencia se realice con el objeto de prestar o solicitar auxilio judicial internacional.

j) Cuando la transferencia se requiera para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

k) Cuando la transferencia sea necesaria en virtud de un contrato celebrado o por celebrar en interés del titular de datos, o cuando se requiera para la ejecución o cumplimiento de un contrato entre el titular y el responsable de datos.

l) Cuando sea necesario adoptar medidas urgentes en materia médica o sanitaria, para la prevención o diagnóstico de enfermedades, para tratamientos médicos o para la gestión de servicios sanitarios o de salud.

La transferencia internacional de datos considera las operaciones de comunicación, transmisión y cesión de datos personales, según la necesidad y finalidades del tratamiento.”.

La Comisión decidió analizar y discutir cada letra del artículo 27.

El Honorable Senador señor Larraín preguntó si es listado es taxativo. Consultó cómo opera la transferencia internacional de datos cuando estamos en presencia de datos sensibles.

El Honorable Senador, señor De Urresti inquirió sobre el principio de reciprocidad.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena manifestó que con el presente título se viene a modernizar la legislación de protección de datos personales. Enfatizó que

hoy en día, la transferencia de datos internacionales no es solo relevante para el desarrollo de la industria, sino que también para las labores de los gobiernos cuando quieren cooperar en materia de fiscalización.

Agregó que para transferir datos, se debe cumplir con las fuentes de licitud para su tratamiento. Asimismo, precisó que la lista de la norma en estudio es taxativa. Sin embargo, adelantó que el artículo siguiente otorga la facultad a la Agencia para autorizar la transferencia internacional de datos, cuando no se verifique ninguna de las circunstancias que exige el presente artículo.

El asesor del Ministerio de Hacienda, señor Godoy sostuvo que la reciprocidad se aplica cuando existen tratados entre países, que establezcan reglas de transferencia e intercambio de datos; o cuando existen convenios de intercambio de información entre organismos públicos y en aquellos programas marco, que configuran reglas a nivel agregado de intercambio de información entre industrias o empresas.

El Honorable Senador señor Larraín propuso incorporar en el inciso primero que se exija que los datos cumplan con los requisitos de licitud de la ley.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena sugirió trasladar el encabezado de la letra a), al inciso primero.

El representante del Ejecutivo, señor Godoy, sugirió la siguiente redacción al encabezado del artículo:

“Artículo 27.- Regla general de autorización. Cumpliéndose los requisitos que de conformidad a esta ley confieren licitud al tratamiento de datos, son lícitas las operaciones de transferencia internacional de datos en los siguientes casos:”.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó esta disposición.

En seguida, se puso en votación la siguiente redacción para su letra a):

“a) Cuando la transferencia se realice a una persona, entidad u organización sujeta al ordenamiento jurídico de un país que proporcione niveles adecuados de protección de datos personales.”

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores De Urresti, Harboe y Larraín, aprobó esta disposición.

En seguida se examinó la letra b) del artículo 27 que dispone:

"b) Cuando la transferencia de datos quede amparada por cláusulas contractuales u otros instrumentos jurídicos suscritos entre el responsable que efectúa la transferencia y el que la recibe y en ellas se establezcan los derechos y garantías de los titulares, las obligaciones de los responsables y los medios de control, o cuando adopten un modelo de cumplimiento o autorregulación vinculante y certificado.".

Respecto a la letra b), **el Presidente de la Comisión, Honorable Senador señor Harboe** hizo presente que la cláusula contractual se establece como fuente de licitud. Preguntó qué ocurre si una empresa chilena ha realizado tratamiento de datos con una finalidad determinada y transfiere los datos a otra empresa ubicada en el extranjero, quien los puede utilizar para una finalidad diversa.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena indicó que debido al caso planteado es importante el encabezado, ya que de ahí se deriva que la licitud tiene relación con la finalidad.

El asesor del Ministerio de Hacienda, señor Godoy hizo presente que la letra b) contempla dos hipótesis. Una corresponde a la transferencia entre dos responsables de datos, mediante un contrato. Agregó que las cláusulas de éste, no solo se refieren a los datos que se entregan de uno a otro, sino que además, en ellas se deben establecer los derechos y garantías de los titulares, las obligaciones de los responsables y los medios de control. La segunda, dice relación con la adopción por parte de los responsables, cuando adopten un modelo de cumplimiento o autorregulación vinculante y certificado.

En esta parte del debate **los representantes del Ejecutivo** sugirieron a la Comisión dividir este precepto en dos letras. Su texto es el siguiente:

"b) Cuando la transferencia de datos quede amparada por cláusulas contractuales u otros instrumentos jurídicos suscritos entre el responsable que efectúa la transferencia y el que la recibe, y en ellas se establezcan los derechos y garantías de los titulares, las obligaciones de los responsables y los medios de control.

c) Cuando el responsable que efectúa la transferencia y el que la recibe, adopten un modelo de cumplimiento o

autorregulación vinculante y certificado de acuerdo a la legislación aplicable para cada uno de ellos.”.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores Araya, Harboe y Larraín, aprobó este cambio de redacción.

En seguida se examinó la letra c) del proyecto de ley, que pasa a ser letra d). Su texto es el siguiente:

“d) Cuando exista consentimiento expreso del titular de datos para realizar una transferencia internacional de datos específica y determinada.”.

Puesta en votación la letra d), fue aprobada por la unanimidad de los Honorables Senadores presentes, señores De Urresti, Harboe y Larraín.

A continuación, la Comisión examinó la nueva letra e). Ella dispone lo siguiente:

“e) Cuando se refiera a transferencias bancarias, financieras o bursátiles específicas y que se realicen conforme a las leyes que regulan estas transferencias.”.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena manifestó que cuando estamos en presencia de operaciones bursátiles, surge lo que se denomina la mensajería *swift*, que corresponde a un mensaje de datos en donde se identifica quién es el comprador, su rut, su cuenta, y ello se traspasa en el mundo de las plataformas electrónicas.

Precisó que la frase: “se realicen de conformidad a su legislación aplicable.”, implica que existen regulaciones que establecen cómo se tienen que entregar esos mensajes.

El Honorable Senador señor Larraín sugirió que se reemplace la expresión: “a su legislación aplicable.”, por “de conformidad a la ley.”.

El Presidente de la Comisión, Honorable Senador señor Harboe, consultó cómo conversa lo anterior con la modificación que se está realizando en materia tributaria, específicamente en lo relacionado con el secreto bancario y la entrega de la información internacional.

El asesor del Ministerio de Hacienda, señor Godoy indicó que la mencionada letra se refiere a transferencia de información en el marco de operaciones financieras o crediticias entre particulares.

El Presidente de la Comisión, Honorable Senador señor Harboe, ratificó que la letra e) dice relación con las transacciones lícitas entre particulares, de conformidad a sus normas particulares de transferencia.

El asesor del Ministerio de Hacienda, señor Godoy hizo presente que tanto la letra d), como la e), se refieren a operaciones que llevan a cabo particulares.

Puesta en votación la letra e), fue aprobada por la unanimidad de los Honorables Senadores presentes, señores De Urresti, Harboe y Larraín.

En seguida, los representantes del Ejecutivo propusieron la aprobación de la siguiente letra e) que pasa a ser letra f)

“e) Cuando la transferencia se efectúe entre sociedades o entidades que pertenezcan a un mismo grupo empresarial, empresas relacionadas o sujetas a un mismo controlador en los términos previstos en la Ley de Mercado de Valores, siempre que todas ellas operen bajo los mismos estándares y políticas en materia de tratamiento de datos personales.”.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena explicó que la Ley de Mercado de Valores, en su artículo 96 y siguientes define lo que se entiende por grupo empresarial.

El Presidente de la Comisión, Honorable Senador señor Harboe planteó el caso de una empresa que pertenece a un holding internacional y ella obtiene el consentimiento para tratar los datos, y otra sociedad, del mismo grupo, le solicita el traspaso de dicha información. Preguntó cómo el sujeto puede reclamar frente al mencionado traspaso.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena indicó que la transferencia debe ser lícita no solo en términos de la fuente de legitimidad, sino que además debe cumplirse con la finalidad. En el caso señalado, no procedería el traspaso.

El Presidente de la Comisión, Honorable Senador señor Harboe sostuvo que como particular se puede perseguir la responsabilidad de la empresa que se encuentra dentro del territorio nacional. Sin embargo, si esta última ha transferido información a su grupo

controlador ubicado en el extranjero, la Agencia de Protección de Datos no tendrá capacidad para fiscalizarlo o sancionarlo.

Aseveró que debiese existir una norma de corresponsabilidad, de lo contrario, podría entenderse que la mencionada norma queda circunscrita solo a las relaciones entre empresas ubicadas en el país.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena remarcó que si el responsable chileno transfiere datos al extranjero, sin cumplir con el principio de finalidad, el titular podrá reclamar ante la empresa chilena.

El Presidente de la Comisión, Honorable Senador señor Harboe preguntó cómo comprueba el titular del dato que fue la empresa nacional la que lo transfirió.

Reiteró que sería necesario implementar una norma de corresponsabilidad en materia de transferencia internacional.

El asesor del Ministerio de Hacienda, señor Godoy manifestó que el titular de datos tiene la posibilidad de ejercer el derecho de acceso, y en virtud de este último, tiene la opción de conocer la información, los datos personales que le conciernen y a quién han sido cedidos.

Agregó que no debiera darse el supuesto que la empresa situada en el extranjero tenga políticas más flexibles de protección de datos, versus la empresa ubicada en Chile, ya que el principio que establece esta regla es que todas estén sujetas al mismo estándar de resguardo y protección de los datos de los titulares. Es decir, no debiera haber estándares de protección distintos.

El Presidente de la Comisión, Honorable Senador señor Harboe, advirtió que a pesar de que los estándares no sean distintos, los objetivos de las empresas pueden ser diferentes.

Inquirió cómo se puede perseguir la responsabilidad de la empresa situada en el extranjero.

El asesor del Ministerio de Hacienda, señor Godoy respondió que la última empresa podrá usar los datos, siempre que esté amparado por algunas de las causales de licitud del tratamiento.

Agregó que cuando se aprobaron las normas sobre cesiones y comunicaciones de datos, se estableció que frente al evento de una cesión ilícita, quien recibe los datos es responsable

solidariamente respecto de los perjuicios que pudiera ocasionar a los titulares de datos y además, lo es de las infracciones.

El asesor del Honorable Senador Larraín, señor Olmedo relató que la cesión transnacional de datos está involucrada en la obligación de transparencia activa del responsable, porque constituye una medida de fiscalización. Enfatizó que debe haber un mecanismo de control, porque la Agencia puede fiscalizar, pero si no hay información sobre la transferencia, se torna muy difícil que el control se produzca en tiempo y forma.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena constató que efectivamente las empresas tienen que informar a quiénes se cedieron los datos. Aseveró que el caso planteado por el Honorable Senador, señor Harboe es complejo porque estamos ante un escenario de extraterritorialidad de la ley.

El Presidente de la Comisión, Honorable Senador señor Harboe señaló que como la Agencia no puede aplicar extraterritorialmente la ley, es imprescindible contar con la corresponsabilidad, para salvaguardar los intereses del titular.

El asesor del Ministerio de Hacienda, señor Godoy constató que luego de la discusión acaecida, se decidió agregar la hipótesis, que consiste en que el responsable podrá eximirse de responsabilidad cuando pruebe que la infracción no le fue imputable.

Como consecuencia de lo anterior, **el representante del Ejecutivo, señor Godoy,** propuso a la Comisión aprobar la siguiente redacción para la letra f)

“f) Cuando la transferencia se efectúe entre sociedades o entidades que pertenezcan a un mismo grupo empresarial, empresas relacionadas o sujetas a un mismo controlador en los términos previstos en la Ley de Mercado de Valores, siempre que todas ellas operen bajo los mismos estándares y políticas en materia de tratamiento de datos personales. El responsable que efectúe la transferencia de datos asumirá la responsabilidad por cualquier infracción a los estándares y políticas corporativas vinculantes en que incurra algunos de los miembros del grupo empresarial. El responsable sólo podrá exonerarse de esta responsabilidad cuando acredite que la infracción no fue imputable al miembro del grupo empresarial correspondiente.”.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó esta disposición.

En seguida, se examinó la letra f) que pasa a ser letra g)

“g) Cuando se deban transferir datos para dar cumplimiento a obligaciones adquiridas en tratados o convenios internacionales que hayan sido ratificados por el Estado chileno y se encuentren vigentes.”

Puesta en votación la letra g), fue aprobada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores De Urresti, Harboe y Larraín.

A continuación se examinó la letra g) que pasa a ser letra h): “h) Cuando la transferencia resulte necesaria por aplicación de convenios de cooperación, intercambio de información o supervisión que hayan sido suscritos por órganos públicos para el cumplimiento de sus funciones y en el ejercicio de sus competencias.”.

Puesta en votación la letra h), fue aprobada por la unanimidad de los Honorables Senadores presentes, señores De Urresti, Harboe y Larraín.

En seguida se puso en discusión la letra h) que pasa a ser letra i). Su texto es el siguiente:

“i) Cuando la transferencia de datos haya sido autorizada expresamente por la ley a un organismo público para el cumplimiento de sus funciones legales.”.

El Honorable Senador señor Larraín hizo presente que lo anterior significará que los organismos mencionados, tendrán la facultad de transferir datos en forma permanente sin ninguna restricción.

El asesor del Ministerio de Hacienda, señor Godoy reconoció que la formulación es muy amplia. Propuso acotarla de la siguiente manera: “Cuando la transferencia de datos haya sido autorizada expresamente por la ley y para un fin específico a un organismo público para el cumplimiento de sus funciones legales.”

Destacó que el organismo requiere una autorización legal expresa para poder transferir datos a un responsable ubicado fuera del territorio nacional. Admitió que se quiere ampliar la hipótesis, a los privados. Consideró que pueden existir particulares que también necesiten transferir datos en virtud de un mandato legal.

En una sesión posterior, el Ejecutivo propuso la aprobación de la siguiente letra i):

“i) Cuando la transferencia de datos realizada por una persona natural o jurídica, pública o privada, haya sido autorizada expresamente por la ley y para una finalidad determinada.”.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó esta disposición.

En seguida, los representantes del Ejecutivo propusieron a la Comisión aprobar las siguientes letra j) y k), nuevas. Su texto es el siguiente:

“j) Cuando la transferencia sea efectuada con el objeto de prestar o solicitar colaboración judicial internacional.

k) Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato entre el titular y el responsable, o para la ejecución de medidas precontractuales adoptadas a solicitud del titular.”.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó ambas letras.

A continuación se examinó la letra l). Su texto es el siguiente:

“l) Cuando sea necesario adoptar medidas urgentes en materia médica o sanitaria, para la prevención o diagnóstico de enfermedades, para tratamientos médicos o para la gestión de servicios sanitarios o de salud.”

Puesta en votación, fue aprobada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores De Urresti, Harboe y Larraín.

Finalmente, la Comisión analizó el inciso final del artículo 27, precepto que dispone lo siguiente:

“La transferencia internacional de datos considera las operaciones de comunicación, transmisión y cesión de datos personales, según la necesidad y finalidades del tratamiento.”.

El asesor del Ministerio de Hacienda, señor Godoy sugirió eliminar este inciso. Explicó que era innecesario en esta normativa.

La Comisión, por la unanimidad de sus miembros presente, Honorables Senadores señores Araya, Harboe y Larraín, acogió este planteamiento.

Artículo 28

A continuación, la Comisión se abocó al estudio del artículo 28 del proyecto de ley del Ejecutivo.

Esta disposición establece las reglas aplicables a países que no poseen niveles adecuados de protección de datos. Su texto es el siguiente:

“Artículo 28.- Reglas aplicables a países que no poseen niveles adecuados de protección de datos. Excepcionalmente, se podrán realizar operaciones específicas de transferencia internacional de datos a personas, entidades u organizaciones sujetas al ordenamiento jurídico de países cuyas legislaciones no cumplan con niveles adecuados de protección de datos, en los siguientes casos:

a) Cuando exista consentimiento expreso del titular de datos para realizar una transferencia o transmisión específica y determinada de datos.

b) Cuando se refiera a transferencias internacionales bancarias, financieras o bursátiles específicas y se realicen conforme a la legislación especial que corresponda.

c) Cuando la transferencia se efectúe entre sociedades o entidades que pertenezcan a un mismo grupo empresarial, empresas relacionadas o sujetas a un mismo controlador de acuerdo a las normas de la ley N° 18.045, de Mercado de Valores, siempre que todas ellas operen bajo los mismos estándares y políticas internas en materia de tratamiento de datos personales.

d) Cuando se deban transferir los datos para dar cumplimiento a obligaciones adquiridas en tratados o convenios internacionales que hayan sido ratificados por el Estado chileno y se encuentren vigentes.

e) Cuando la transferencia resulte necesaria por la aplicación de convenios de cooperación, intercambio de información o

supervisión que hayan sido suscritos por los órganos del Estado para el cumplimiento de sus funciones y en el ejercicio de sus competencias.

f) Cuando la transferencia o el intercambio de datos haya sido autorizado expresamente por la ley a un organismo público para el cumplimiento de sus funciones legales.

g) Cuando se haga con el objeto de prestar o solicitar auxilio judicial internacional.

h) Cuando sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

i) Cuando sea necesario adoptar medidas urgentes en materia médica o sanitaria, para la prevención o diagnóstico de enfermedades, para tratamientos médicos o la gestión de servicios de salud.

Los responsables deberán informar previamente y en forma electrónica a la Agencia de Protección de Datos Personales la transferencia o transmisión internacional de datos.

En todos aquellos casos en que sea posible, las operaciones de transferencia o transmisión internacional de datos deberán quedar amparadas por cláusulas contractuales que establezcan los derechos y garantías de los titulares y las obligaciones de los responsables.

Cuando no se verifique ninguna de las circunstancias señaladas en las letras anteriores, la Agencia de Protección de Datos Personales podrá autorizar la transferencia o transmisión internacional de datos, siempre que el transmisor y el receptor de los datos otorguen las garantías adecuadas en relación con la protección de los derechos de las personas que son titulares de estos datos. La Agencia de Protección de Datos Personales podrá imponer condiciones previas para que se verifique la transferencia.”

Al comenzar el estudio de esta materia, **los representantes del Ejecutivo, señora Piedrabuena y señor Godoy**, plantearon a la Comisión aprobar el texto del proyecto de ley del Ejecutivo, enmendado en los siguientes términos:

“Artículo 28.- Regla de determinación de países adecuados y demás normas aplicables a la transferencia internacional de datos. Se entiende que el ordenamiento jurídico de un país posee niveles adecuados de protección de datos, cuando cumple con estándares similares o superiores a los fijados en esta ley. La Agencia de Protección de Datos Personales determinará los países que poseen niveles adecuados de protección de datos, considerando a los menos, lo siguiente:

a) El establecimiento de los principios que rigen el tratamiento de los datos personales;

b) La existencia de normas que reconozcan y garanticen los derechos de los titulares de datos y de una autoridad pública de control o tutela;

c) La imposición de obligaciones de información y seguridad a los responsables del tratamiento de los datos, y

d) La determinación de responsabilidades en caso de infracciones.

En todos aquellos casos que no correspondan a los señalados en las letras a) y b) del artículo anterior y, en tanto sea posible, las operaciones de transferencia internacional de datos deberán quedar amparadas por cláusulas contractuales que establezcan los derechos y garantías de los titulares y las obligaciones de los responsables. La Agencia de Protección de Datos Personales en su página web pondrá a disposición de los interesados modelos tipo de instrumentos y cláusulas contractuales para la transferencia internacional de datos.

Cuando no se verifique ninguna de las circunstancias señaladas en el artículo anterior, la Agencia de Protección de Datos Personales podrá autorizar la transferencia internacional de datos, siempre que el transmisor y el receptor de los datos otorguen las garantías adecuadas en relación con la protección de los derechos de las personas que son titulares de estos datos y la seguridad de la información transferida. La Agencia de Protección de Datos Personales podrá imponer condiciones previas para que se verifique la transferencia.

Corresponderá al responsable de datos que efectuó la transferencia internacional de datos, acreditar que ésta se practicó de conformidad a las reglas establecidas en esta ley.”.

El asesor del Ministerio de Hacienda, señor Godoy precisó que el artículo corresponde a una especificación de la letra a) del artículo 27. Agregó que en este precepto se establecen criterios generales para efectos de adoptar una decisión lo más técnica posible al momento de determinar cuál es el listado de países adecuados.

Manifestó que la letra a) del presente artículo, busca analizar los principios que rigen el tratamiento de los datos personales, y no ceñirse a un catálogo determinado.

Asimismo, hizo presente que en Estados Unidos de Norteamérica no existe autoridad administrativa de control, pero sí cuentan con una autoridad judicial. Por lo tanto, esta disposición no se puede circunscribir a un solo tipo de autoridad.

El asesor del Honorable Senador Larraín, señor Olmedo planteó que se incorpore la opción de que la Agencia dicte una resolución fundada cuando exista alguna duda. Expresó que la mencionada Agencia está dotada de esa facultad.

El Honorable Senador señor Larraín manifestó que tanto las autoridades jurisdiccionales como las administrativas, son públicas. Preguntó si existe la necesidad de diferenciarlas.

El asesor del Ministerio de Hacienda, señor Godoy, sostuvo que tener una regla más precisa en esta materia genera mayor certeza, para efectos de evitar discrecionalidades.

En una sesión posterior de la Comisión, **los representantes del Ejecutivo, señora Piedrabuena y señor Godoy**, sugirieron introducir una serie de cambios a la norma en estudio. Estos son los siguientes:

- “Para agregar en el inciso primero, luego de la palabra “determinará” la expresión “fundadamente”.”.

Al explicar este cambio, **el asesor del Ministerio de Hacienda, señor Godoy,** manifestó que esta modificación obedece a una solicitud de la Comisión.

- Para reemplazar la letra b) del artículo 28 por la siguiente:

“b) La existencia de normas que reconozcan y garanticen los derechos de los titulares de datos y la existencia de una autoridad pública jurisdiccional o administrativa de control o tutela;”

Al justificar esta enmienda, **el asesor del Ministerio de Hacienda, señor Godoy,** sostuvo que en la propuesta original solo hablaba de autoridad pública de control o tutela. Observó que es importante que se recalque que se refiere a una autoridad pública jurisdiccional o administrativa.

Recalcó que lo importante es que exista un sistema jurídico que garantice los derechos de las personas y una autoridad judicial o administrativa de carácter independiente que pueda asegurar el ejercicio de estos derechos.

-Seguidamente, propuso reemplazar el inciso segundo por el siguiente:

“La Agencia de Protección de Datos Personales pondrá en su página web a disposición de los interesados modelos tipo de cláusulas contractuales y otros instrumentos jurídicos para la transferencia internacional de datos.”

El asesor del Ministerio de Hacienda, señor Godoy aclaró que esta nueva propuesta del Ejecutivo busca simplificar el inciso segundo. Se acogió la idea de que la Agencia disponga de modelos que contengan cláusulas contractuales e instrumentos jurídicos que puedan actuar como guía para la transferencia internacional de datos.

Concluidas estas explicaciones, el Presidente de la Comisión, Honorable Senador señor Harboe, puso en votación los incisos primero y segundo del artículo 28, con las modificaciones planteadas por los representantes del Ejecutivo.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó estas disposiciones con las reseñadas enmiendas.

A continuación, puso en votación los incisos tercero y cuarto del artículo 28.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores De Urresti, Harboe y Larraín, aprobó estos preceptos.

El texto acordado precedentemente fue ratificado mediante una indicación que presentó el Ejecutivo, la que se dio por aprobada con las votaciones señaladas precedentemente.

Artículo 29

A continuación, la Comisión examinó el artículo 29 contenido en el proyecto de ley del Ejecutivo.

Mediante esta disposición se agrega un artículo nuevo a la ley N° 19.628, con el propósito de precisar los casos en que proceden las exclusiones, comunicaciones y ciertas atribuciones de fiscalización de la Agencia de protección de datos.

El texto de esta norma es el siguiente:

“Artículo 29.- Exclusiones, comunicaciones y fiscalización.- No se considera transferencia internacional de datos personales cuando un responsable efectúa operaciones de tratamiento a través de un tercero sujeto a la legislación de otro país, siempre que ese tercero efectúe las operaciones de tratamiento por encargo y bajo las instrucciones del responsable de datos de acuerdo a lo establecido en el artículo 15 bis de esta ley.

El mandato o encargo señalado en el inciso anterior deberá constar a través de un contrato escrito. La realización de estas operaciones deberá ser comunicada previamente y en forma electrónica a la Agencia de Protección de Datos Personales.

La Agencia de Protección de Datos Personales fiscalizará las operaciones de transferencia o transmisión internacional de datos, pudiendo formular recomendaciones, adoptar medidas conservativas y en casos calificados, suspender temporalmente el envío de los datos.”.

Al comenzar el análisis de este precepto, los representantes del Ejecutivo, señora Piedrabuena y señor Godoy, sugirieron a la Comisión aprobar el proyecto de ley del Ejecutivo, enmendado en los siguientes términos:

“Artículo 29.- Fiscalización.- La Agencia de Protección de Datos Personales fiscalizará las operaciones de transferencia internacional de datos, pudiendo formular recomendaciones, adoptar medidas conservativas y en casos calificados, suspender temporalmente el envío de los datos.”.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores De Urresti, Harboe y Larraín, concordó con este cambio y lo aprobó sin enmiendas.

-.-.-

En una sesión posterior, la Comisión analizó la propuesta, contenida en el proyecto de ley del Ejecutivo, para incorporar los siguientes Títulos VI, VII y VIII, nuevos, a la ley N° 19.628. En estos apartados se determina la organización, funciones, atribuciones de la Agencia de Protección de Datos Personales, los distintos tipos de infracciones a las disposiciones que establece este proyecto de ley y las sanciones que se pueden aplicar.

Artículo 30

Este precepto del proyecto de ley del Ejecutivo encabeza el nuevo Título VI de la mencionada ley. En él se crea a la Agencia de Protección de Datos Personales y se definen sus características institucionales. Su texto es el siguiente:

"Artículo 30.- Agencia de Protección de Datos Personales. Créase la Agencia de Protección de Datos Personales, organismo público, de carácter técnico, descentralizado, con personalidad jurídica y patrimonio propio, encargado de velar por el cumplimiento de la normativa relativa al tratamiento de los datos personales y su protección, sometido a la supervigilancia del Presidente de la República a través del Ministerio de Hacienda y afecto al Sistema de Alta Dirección Pública establecido en la ley N° 19.882.

El domicilio de la Agencia de Protección de Datos Personales será la ciudad de Santiago.".

Al iniciarse el estudio de este precepto, **los representantes del Ejecutivo, señora Piedrabuena y señor Godoy**, propusieron a la Comisión aprobar el proyecto del Ejecutivo, enmendado en los siguientes términos:

"Artículo 30.- Agencia de Protección de Datos Personales. Créase la Agencia de Protección de Datos Personales, organismo público descentralizado, de carácter técnico, con personalidad jurídica y patrimonio propio, **independiente de todo órgano o servicio**, sometido a la supervigilancia del Presidente de la República a través del Ministerio de Hacienda, encargado de velar por el cumplimiento de la normativa relativa al tratamiento de los datos personales y su protección.

El domicilio de la Agencia de Protección de Datos Personales será la ciudad de Santiago.".

Al explicar esta nueva redacción **El asesor del Ministerio de Hacienda, señor Godoy** manifestó que la Agencia constituye el órgano que tiene a su cargo el cumplimiento de la norma relativa al tratamiento de los datos personales y su protección.

Agregó que los cambios más sustanciales de la propuesta del Ejecutivo, dicen relación con haber recogido las opiniones vertidas en las audiencias previas, con la finalidad de reforzar el carácter autónomo de la mencionada institución.

Expresó que cuando se habla de autonomía, nos hacemos cargo de la autonomía de carácter administrativo, y no de la política. Destacó que Chile es un país unitario.

Recordó que el Gobierno está compuesto por el Presidente de la República y sus Ministros, y en el ámbito territorial, por los Intendentes y Gobernadores.

Añadió que la Administración del Estado está constituida por un complejo orgánico de instituciones que se encuentran bajo la dependencia o bajo la tutela del Presidente de la República.

Subrayó que es en el ámbito de la Administración del Estado donde se radica la Agencia. Desde el punto de vista normativo, declaró que ella se acerca a un modelo institucional similar al de la Fiscalía Nacional Económica. Esta última es parte de la Administración del Estado, se relaciona con el Presidente de la República, a través del Ministerio de Economía, y se encuentra bajo la supervigilancia de la máxima autoridad, mas no bajo su potestad jerárquica.

Aseveró que los criterios para establecer la autonomía de un órgano de la Administración del Estado, son los siguientes:

- Servicio descentralizado (personalidad jurídica y patrimonio propio);

- Dependencia de la autoridad del servicio, sea unipersonal o colegiada, con el Presidente de la República (nombramiento y remoción) y participación de otros Poderes del Estado, Senado o Corte Suprema;

- Revisión de las actuaciones y decisiones de la autoridad del servicio; y

- Gestión presupuestaria.

Continuó señalando que estamos ante una Agencia, cuyo nombramiento depende del Presidente de la República, a través de la Alta Dirección Pública y la remoción de sus miembros está determinada por causales específicas. Connotó que en ella participa la Corte Suprema.

Respecto a la autonomía técnica, observó que estamos ante un órgano que no está sujeto a ninguna otra autoridad.

Aseveró que la Agencia cuenta con patrimonio propio. Por lo tanto, goza de autonomía en la administración del presupuesto que le fije la ley.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena agregó que el período de duración en el cargo del Director/a se fijó en 5 años, para otorgarle mayor autonomía a la Agencia, desacoplándolo del ciclo político.

El Presidente de la Comisión, Honorable Senador señor Harboe, afirmó que el objetivo de la presente iniciativa consiste en mejorar el nivel de protección de los datos personales de los ciudadanos. Agregó que lo anterior implica que en la transferencia internacional de datos, Chile sea considerado un país seguro.

Constató que algunos abogados y miembros del Consejo para la Transparencia han manifestado su preocupación, porque la actual propuesta regulatoria no reuniría las condiciones necesarias para que Chile sea considerado un país seguro, de acuerdo a los estándares de la Unión Europea.

Solicitó que el Ejecutivo entregue los argumentos por los cuales se asegure que el presente proyecto cumple con los niveles de autonomía suficiente para ser considerado un país seguro en materia de protección de datos.

Consignó que fruto de un encuentro organizado por la Comisión Bicameral Pro Transparencia y Probidad, se recibió al señor Director del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), de México, quien expuso sobre su experiencia. En esa instancia planteó la idea de partir con una Agencia de Protección de Datos y luego, en el camino, decidir si se incorpora al Consejo para la Transparencia en la función de protección.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena sostuvo que no comprende en qué se basan las aseveraciones vertidas respecto a que la Agencia no cumpliría con los estándares de la Comunidad Europea.

Manifestó que el órgano que se sugiere crear, cumple con todos los principios del Reglamento de la Unión Europea en materia de protección de datos. Agregó que cada gobierno es soberano de establecer sus propias instituciones de acuerdo al ordenamiento jurídico interno.

Los mencionados principios consisten en que la autoridad de control cuente con total independencia en el desempeño de sus

funciones en el ejercicio de los poderes, de conformidad a la ley que la crea. Recalcó que la institución que se propone instituir es un órgano descentralizado que no depende jerárquicamente de ningún ministerio, pero queda bajo la supervigilancia del Presidente de la República.

Otro principio dispone que él o los miembros que formen parte de la autoridad de control deben estar ajenos de presiones en el desempeño de su ejercicio. Ello se resguarda por el proceso de nombramiento y por la configuración de causales taxativas de remoción.

Precisó que el mencionado reglamento también prescribe que él o los miembros de cada autoridad de control deben abstenerse de cualquier acción que sea incompatible con sus funciones. Subrayó que ello está recogido en la iniciativa en estudio y recoge una regla que se aplica a otras agencias estatales que tienen una naturaleza parecida. Asimismo, aseveró, se le proporcionan los medios económicos y técnicos para poder funcionar.

En cuanto al nombramiento de la autoridad de control, agrega el Reglamento, debe ser transparente y establecido por ley. Agrega que cada miembro debe poseer la experiencia, las aptitudes y los conocimientos adecuados. En la propuesta del Ejecutivo, la designación se lleva a cabo mediante el mecanismo de la Alta Dirección Pública. Asimismo se establecen las causales por las que estos funcionarios pueden cesar en sus funciones y en qué condiciones pueden ser destituidos.

Consignó que los principios establecidos en el proyecto son muy similares a los fijados por la Red Iberoamericana de Protección de Datos.

Reiteró que en la normativa que se sugiere, se está dando cumplimiento a cada uno de los principios mencionados.

Recordó que el Director del INAI de México advirtió que el peor error que podríamos hacer en Chile es seguir el ejemplo mexicano, que consistió en tener en una sola autoridad tanto para el acceso a la información como para la protección de los datos personales.

Seguidamente, afirmó que existe un informe elaborado por la Universidad de Chile del año 2010 que se pronuncia sobre las ventajas e inconvenientes del hecho de establecer en una sola agencia ambas funciones. Connotó que la principal desventaja dice relación con que los bienes jurídicos protegidos son contrapuestos.

Recalcó que el establecer ambas funciones en un mismo organismo, provoca una desprotección del ciudadano. Señaló que en el mencionado informe se establece que la ventaja de que se cree un solo

órgano, lo constituyen los costos y la eficiencia económica. Lo anterior no sería efectivo, puesto que el Consejo para la Transparencia, en caso de hacerse cargo de la protección de datos personales, estaría exigiendo más recursos de los que se detallan en el informe financiero en relación a la creación de la Agencia de Protección de Datos Personales.

El asesor del Comité Udi, señor Mery, constató que en el grupo de asesores parlamentarios ha habido, respecto de la Agencia de Protección de Datos Personales, una división de pareceres. Estimó que hay muy buenos argumentos para creer que existen otras formas de organización que son más eficientes y más eficaces que las propuestas por el Ejecutivo.

Aseveró que el ideal de un órgano que cuente con autonomía y con una estructura de gobierno con un Director y un Consejo Directivo no aparece recogido en la propuesta del Ejecutivo.

Sostuvo que no es fácil diseñar un mecanismo de gobierno corporativo. Dado lo anterior, señaló que surge como opción razonable, radicar esta competencia en el Consejo para la Transparencia. Indicó que se ha dicho que la función y orientación dogmática del Consejo, tendería a privilegiar la publicidad por sobre la protección de datos. Hizo presente que la anterior afirmación es revisable de acuerdo con la jurisprudencia que emana de dicho Consejo o de los tribunales de justicia que han tenido que revisar cuestiones de esta naturaleza.

Constató que existe una jurisprudencia robusta y explícita del Consejo que se debiera considerar en esta materia.

Expuso que no cree que la especialidad diferente que se identifica entre el Consejo y la Agencia, constituya un obstáculo. Añadió que si hubiese decisiones del Consejo que pudieran afectar derechos, en último término, podrá recurrirse a los tribunales de justicia.

Destacó que es rebatible la afirmación que se ha dado de que la mencionada Agencia asegura una protección más eficaz.

Observó que la relación de la Agencia con el Ministerio de Hacienda aminorará la autonomía de ella.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena, recordó que el inciso primero del artículo 1° de la Ley sobre acceso a la información pública, dispone:

“Artículo 1°.- La presente ley regula el principio de transparencia de la función pública, el derecho de acceso a la información de los órganos de la Administración del Estado, los procedimientos para el

ejercicio del derecho y para su amparo, y las excepciones a la publicidad de la información.”.

Agregó que el artículo 33, letra m) del citado cuerpo legal dispone que el Consejo para la Transparencia tendrá las siguientes funciones y atribuciones:

“m) 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.”.

Lo anterior, implica concluir que al dictarse dicho cuerpo legal, se pensó en que dicha tarea correspondería al Consejo. Aseveró que posteriormente se llegó a la conclusión que no constituía el camino correcto.

Finalmente, consignó que existe jurisprudencia que permite afirmar que la Agencia ha privilegiado el acceso a la información, por sobre la protección de datos.

Seguidamente, **el asesor del Ministerio de Hacienda, señor Godoy,** precisó que la autonomía, puede ser de carácter constitucional o legal.

Agregó que el Consejo para la Transparencia posee un estándar de autonomía legal. Declaró que, desde el punto de vista de la relación con el Presidente de la República, las autonomías legales pueden ser de dos tipos, a saber, que se vinculen directamente con él, como ocurre con el Consejo de Defensa del Estado, y otra, que se trate de órganos con autonomía, pero que se relacionan con la máxima autoridad de la Nación a través de un Ministerio. Añadió que todos los órganos autónomos, a excepción del Consejo de Defensa del Estado, se unen con el Presidente de la República, a través de un Ministerio.

Destacó que lo anterior no significa que el Director de la Agencia sea un funcionario que esté bajo la dependencia de un Ministerio, sino que está bajo la supervigilancia del Presidente de la República. Mencionó que dicho funcionario se relaciona administrativamente con el Ministerio de Hacienda.

Luego, hizo presente que España acaba de actualizar su legislación en materia de protección de datos. Expresó que el modelo de la Agencia Española consiste en una autoridad administrativa independiente del ámbito estatal, de las previstas en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, con personalidad jurídica y plena capacidad pública y privada, que actúa con plena independencia de los

poderes públicos en el ejercicio de sus funciones y que se relaciona con el Gobierno a través del Ministerio de Justicia.

Consignó que la autoridad que se propone, es autónoma en el mecanismo de nombramiento y de remoción. Agregó que no está sujeta a la jerarquía ni a la decisión arbitraria de la máxima autoridad.

Indicó que las decisiones de la Agencia Nacional de Protección de Datos, no están subordinadas a ninguna potestad administrativa de revisión, y solo están sujetas al control jurisdiccional.

Respecto al gobierno corporativo, estimó que una autoridad colegiada no implica mayor calidad técnica, ni mejores decisiones. Ello dice relación exclusivamente con el marco institucional.

Finalmente, reconoció que tras revisar exhaustivamente las opciones institucionales disponibles, se optó por el modelo mayoritario en el mundo, a saber, que el acceso a la información y la protección de datos estén bajo órganos distintos.

El Presidente de la Comisión, Honorable Senador señor Harboe, sostuvo que dentro de la Comisión existen diferentes visiones sobre el tema que se está discutiendo, todas muy legítimas.

Hizo presente que lo importante es que, desde el punto de vista práctico, se cumpla con los estándares de las diferentes instituciones que hoy en día establecen principios, tales como la Unión Europea, Apec, etcétera.

En relación a la autonomía, ésta no es sinónimo de independencia. Relató que nuestra Carta Fundamental cuenta con órganos de carácter autónomo, que operan sobre la base del poder decisorio, que es independiente de la autoridad política. Ejemplos de ello lo constituye el Consejo de Defensa del Estado, la Fiscalía Nacional Económica.

Subrayó que la clave en esta materia está dada por el hecho de que el nombramiento de su Director y las causales de remoción están establecidas por ley. Unido a lo anterior, agregó, la Agencia debe tener un grado de independencia del poder político.

Luego, añadió que las decisiones de esta última no serán susceptibles de recursos jerárquicos. Como consecuencia de ello, un ciudadano que se sienta afectado por una decisión no podrá recurrir ante el Ministro de Hacienda. Sin embargo, podrá presentar el o los recursos judiciales correspondientes.

Argumentó que, desde el punto de vista del presupuesto, al Congreso le corresponde aprobar la norma. Estimó que, desde el punto de vista de la autonomía, no hay mayor conflicto.

Destacó que la discusión pendiente consiste en determinar el órgano que debe conocer de la protección de datos.

Hizo presente que cada vez que se realiza una transacción económica existe un flujo de datos que pueden afectar derechos. Por lo tanto, los ciudadanos requieren de un mecanismo y de una autoridad de protección. Otorgarle esa responsabilidad al mencionado Consejo, puede significar poner en riesgo la función que ha desarrollado éste, y ello puede constituir una afectación de la democracia.

Se mostró partidario de llevar a cabo el perfeccionamiento de esta institución desde el punto de vista del gobierno corporativo.

Sugirió consagrar en el artículo en estudio un término que otorgue mayor tranquilidad a aquellos que puedan tener dudas respecto de la autonomía.

En una sesión posterior, **el Ejecutivo** presentó una indicación para sustituir la redacción de este precepto por la siguiente:

“Articulo 30. - Agencia de Protección de Datos Personales. Créase la Agencia de Protección de Datos Personales, organismo público autónomo, descentralizado, de carácter técnico, con personalidad jurídica y patrimonio propio, sometido a la supervigilancia del Presidente de la República a través del Ministerio de Hacienda, encargado de velar por el cumplimiento de la normativa relativa al tratamiento de los datos personales y su protección. La Agencia estará afecta al Sistema de Alta Dirección Pública, sin perjuicio de las normas que se establecen en esta ley.

El domicilio de la Agencia de Protección de Datos Personales será la ciudad de Santiago.”.

El señor Presidente de la Comisión valoró esta redacción pues incorpora la expresión “autónomo”, de manera que se consagra la autonomía legal del órgano.

Consideró relevante que cuando se discuta las funciones y atribuciones, se analice la institución desde el prisma de una mirada eminentemente técnica. Constató que se necesitarán expertos en

estas materias, que entiendan el equilibrio que debe existir entre el flujo de datos y la protección de los derechos de los titulares de datos.

El asesor del Ministerio de Hacienda, señor Godoy agregó que en la redacción original se señalaba que la Agencia estaba afecta al sistema de Alta Dirección Pública. Reseñó que con posterioridad se sugirió eliminarlo, porque se reguló en otro artículo el nombramiento del Director de la Agencia mediante ese procedimiento.

La nueva propuesta del Ejecutivo consiste en reincorporar, al final del inciso primero, la siguiente frase: “La Agencia estará afecta al Sistema de Alta Dirección Pública, sin perjuicio de las normas que se establecen en esta ley.”.

Explicó que el Director de la Agencia será elegido mediante un procedimiento especial en el que participa el Senado, entre otros. Añadió que el segundo nivel jerárquico también sigue afecto al sistema de Alta Dirección Pública.

El Presidente de la Comisión, Honorable Senador señor Harboe declaró cerrado el debate y puso en votación el artículo 30

La Comisión, por la unanimidad de sus miembros presente, Honorables Senadores señores Araya, De Urresti, Harboe y Larraín, aprobó la indicación del Ejecutivo.

Artículo 31

En seguida, la Comisión consideró el artículo 31 del proyecto de ley del Ejecutivo, disposición que establece las funciones y atribuciones de la Agencia de Protección de Datos Personales. Su texto es el siguiente:

“Artículo 31.- Funciones y atribuciones. La Agencia de Protección de Datos Personales tendrá las siguientes funciones y atribuciones:

a) Dictar instrucciones y normas generales y obligatorias con el objeto de regular las operaciones de tratamiento de datos personales conforme a los principios establecidos en esta ley, salvo aquellos tratamientos de datos regidos por leyes especiales y sujetos a la potestad normativa de otro órgano público. Las instrucciones y normas generales que dicte la Agencia de Protección de Datos Personales deberán ser emitidas previa consulta pública efectuada a través de la página web institucional.

b) Prestar asistencia técnica, cuando le sea requerida, al Congreso Nacional, al Poder Judicial, a la Contraloría General de la República, al Ministerio Público, al Tribunal Constitucional, al Banco Central, al Servicio Electoral, a la Justicia Electoral y los demás tribunales especiales creados por ley, en la dictación y ejecución de las políticas y normas internas de estos organismos, con el objeto que sus operaciones y actividades de tratamiento de datos personales se realicen conforme a los principios y obligaciones establecidos en esta ley.

c) Fiscalizar el cumplimiento de las disposiciones de esta ley respecto de las operaciones y actividades de tratamiento de datos personales.

d) Requerir a quienes realicen tratamiento de datos personales la información que fuere necesaria para el cumplimiento de sus funciones normativas y fiscalizadoras.

e) Resolver los reclamos que formulen los titulares de datos en contra de los responsables de datos por infracción a esta ley, sus reglamentos o las instrucciones y normas generales dictadas por la Agencia de Protección de Datos Personales.

f) Ejercer la potestad sancionadora sobre las personas naturales o jurídicas, salvo los órganos públicos, que traten datos personales con infracción a esta ley e imponer las sanciones establecidas en ella.

g) Determinar las infracciones e incumplimientos en que incurran los órganos públicos en sus operaciones de tratamiento de datos, respecto de los principios y obligaciones establecidos en esta ley.

h) Requerir a la Contraloría General de la República que instruya los procedimientos administrativos competentes con el objeto de establecer las responsabilidades administrativas y aplicar las sanciones respectiva, al jefe superior del órgano público y a sus funcionarios, según corresponda, por infracción a los principios y obligaciones establecidos en esta ley.

i) Desarrollar programas, proyectos y acciones de difusión, promoción e información a la ciudadanía, en relación al respeto y protección del derecho a la vida privada y a la protección de sus datos personales.

j) Colaborar con los órganos públicos en el diseño e implementación de políticas y acciones destinadas a velar por la protección de los datos personales y su correcto tratamiento.

k) Celebrar convenios de cooperación y prestación de servicios con órganos públicos y desarrollar programas de asistencia técnica.

l) Participar, recibir cooperación y colaborar con organismos públicos internacionales en materias propias de su competencia.

m) Solicitar la representación judicial de sus intereses al Consejo de Defensa del Estado de conformidad a la ley.

n) Certificar, registrar y supervisar los modelos de prevención de infracciones y los programas de cumplimiento y administrar el Registro Nacional de Cumplimiento y Sanciones.

o) Ejercer las demás funciones y atribuciones que la ley le encomiende.”.

Al iniciarse el estudio de este precepto, **los representantes del Ejecutivo, señora Piedrabuena y señor Godoy**, propusieron aprobar el texto del proyecto del Ejecutivo, enmendado en los siguientes términos:

“Artículo 31.- Funciones y atribuciones. La Agencia de Protección de Datos Personales tendrá las siguientes funciones y atribuciones:

a) Aplicar e interpretar administrativamente las disposiciones legales y reglamentarias cuyo cumplimiento le corresponde vigilar, e impartir instrucciones de carácter general a las personas naturales o jurídicas que realicen tratamiento de datos personales. Las instrucciones generales que dicte deberán ser emitidas previa consulta pública efectuada a través de su página web institucional.

b) Fiscalizar y velar por el cumplimiento de los principios, derechos y obligaciones establecidos en esta ley. Para tales efectos, podrá solicitar la entrega de cualquier documento, libro o antecedente que sea necesario.

c) Resolver las solicitudes y reclamaciones que formulen los titulares en contra de los responsables de datos.

d) Investigar y determinar las infracciones en que incurran los responsables de datos y ejercer, en conformidad a la ley, la potestad sancionatoria. Para tales efectos, podrá citar a declarar, entre otros, al titular, a los representantes legales, administradores, asesores y dependientes del responsable de datos, así como a toda persona que haya tenido participación o conocimiento respecto de algún hecho que sea

relevante para resolver un procedimiento sancionatorio. Asimismo, podrá tomar las declaraciones respectivas por otros medios que aseguren su fidelidad.

e) Adoptar las medidas preventivas o correctivas que disponga la ley.

f) Proponer al Presidente de la República, por intermedio del Ministerio de Hacienda, las normas legales y reglamentarias para asegurar a las personas la debida protección de sus datos personales y perfeccionar la regulación sobre el tratamiento y uso de esta información.

g) Relacionarse con los organismos públicos y con los demás órganos del Estado, en el marco de sus funciones y competencias legales.

h) Desarrollar programas, proyectos y acciones de difusión, educación, promoción e información dirigidos a la ciudadanía y a los responsables de datos, en relación al respeto y protección del derecho a la vida privada y a la protección de los datos personales.

i) Prestar asistencia técnica, cuando le sea requerida, al Congreso Nacional, al Poder Judicial, a la Contraloría General de la República, al Ministerio Público, al Tribunal Constitucional, al Banco Central, al Servicio Electoral, a la Justicia Electoral y los demás tribunales especiales creados por ley, para la dictación y ejecución de las políticas y normas internas de estos organismos sobre el tratamiento y la protección de los datos personales.

j) Colaborar con los órganos públicos en el diseño e implementación de políticas, programas y acciones destinadas a velar por la protección de los datos personales y su correcto tratamiento.

k) Celebrar convenios o memorandos de entendimiento con organismos nacionales, internacionales o extranjeros, sean estos públicos o privados y desarrollar programas de asistencia técnica.

l) Participar, recibir cooperación y colaborar con organismos internacionales en materias propias de su competencia.

m) Solicitar la representación judicial de sus intereses al Consejo de Defensa del Estado de conformidad a la ley.

n) Certificar, registrar y supervisar los modelos de prevención de infracciones y los programas de cumplimiento y administrar el Registro Nacional de Cumplimiento y Sanciones.

o) Resolver las solicitudes y controversias que se susciten sobre si una determinada base de datos o conjunto de datos es considerada fuente de acceso público e identificar categorías genéricas, clases o tipos de datos, conjuntos de datos o bases de datos que posean esta condición.

p) Ejercer las demás funciones y atribuciones que la ley le encomiende.”

Al comenzar el análisis de esta nueva redacción planteada por el Ejecutivo, **el Presidente de la Comisión, Honorable Senador señor Harboe**, sugirió a la Comisión considerar separadamente cada una de las letras de este precepto.

En primer lugar, sometió a discusión el encabezado y la letra a) del artículo 31. Su texto es el siguiente:

“Artículo 31.- Funciones y atribuciones. La Agencia de Protección de Datos Personales tendrá las siguientes funciones y atribuciones:

a) Aplicar e interpretar administrativamente las disposiciones legales y reglamentarias cuyo cumplimiento le corresponde vigilar, e impartir instrucciones de carácter general a las personas naturales o jurídicas que realicen tratamiento de datos personales. Las instrucciones generales que dicte deberán ser emitidas previa consulta pública efectuada a través de su página web institucional.”.

En primer lugar, intervino **el asesor del Ministerio de Hacienda, señor Godoy,** quien manifestó que esta letra responde a la atribución más genérica de la Agencia y dice relación con la facultad de poder aplicar e interpretar administrativamente la ley en materia de protección y tratamiento de datos personales. Asimismo, se le otorga la potestad de dictar instrucciones de carácter general, con el objeto de lograr la aplicación de la ley.

Destacó que siguiendo los estándares de la OCDE, las instrucciones que genere la Agencia, se deben someter a un proceso de consulta pública.

El asesor del Comité Udi, señor Mery expresó que a raíz de la reciente tramitación de la ley que modifica la ley N° 19.496, sobre Protección de los Derechos de los Consumidores, se estableció que las instrucciones son vinculantes para el Sernac o para las instituciones públicas que realicen tratamiento de datos personales.

Agregó que en la letra en estudio se señala que la Agencia está facultada para impartir instrucciones de carácter general a las personas naturales o jurídicas que realicen tratamiento de datos personales, sin importar que sean públicos o privados.

Consideró importante conocer la opinión del Ejecutivo, acerca de si convendría adoptar un régimen regulatorio similar al consagrado en la ley que modifica la ley N° 19.496.

El Presidente de la Comisión, Honorable Senador señor Harboe, indicó que tiene una diferencia importante con lo planteado. Añadió que en cada operación que uno realiza, se genera un flujo de datos personales. Consignó que la afectación principal de los ciudadanos dice relación con la acción privada en materia de datos personales.

Sostuvo que la administración pública también debe modernizarse. Estimó que la norma en estudio es adecuada. Expuso que es partidario que la Agencia sea el intérprete exclusivo de la ley, para que solo el especialista en la materia pueda interpretarla.

Desde el punto de vista de la aplicación, se opuso a excluir a las personas jurídicas privadas, porque debe haber uniformidad de criterios en esta materia.

Preguntó qué ocurriría si excluyéramos a estas últimas, qué certeza tendría la propia industria si no tuviese la Agencia, la mencionada facultad de interpretación.

Recalcó que, por regla general, se debe evitar la judicialización, y para ello debe mantenerse el criterio que inspira la norma, porque protege al titular y da certeza a la industria que desarrolla el tratamiento de datos personales.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena, subrayó que la norma se aplica tanto a responsables privados como públicos, a excepción de los organismos autónomos constitucionales, entidades que no están sometidas a los dictados de la Agencia.

Puesta en votación la letra a) del artículo 31, fue aprobada con el voto favorable de los Honorables Senadores señores De Urresti y Harboe. Se abstuvo, el Honorable Senador, señor Moreira.

A continuación, **el señor Presidente de la Comisión**, sometió a debate lo preceptuado en la letra b) del artículo 31. Su texto es el siguiente:

“b) Fiscalizar y velar por el cumplimiento de los principios, derechos y obligaciones establecidos en esta ley. Para tales efectos, podrá solicitar la entrega de cualquier documento, libro o antecedente que sea necesario.”

El Presidente de la Comisión, Honorable Senador señor Harboe precisó que la facultad que se establece en esta letra, que es bastante amplia, trae aparejado un conjunto de responsabilidades para la Agencia.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena aseveró que en el artículo 50 se consagra el deber de los funcionarios de reserva y confidencialidad.

El asesor del Comité Udi, señor Mery aclaró que la solicitud de entrega de cualquier documento, libro o antecedente, prescrita en la letra en estudio, se refiere a los entes que están siendo fiscalizados.

El Presidente de la Comisión, Honorable Senador señor Harboe, recordó que la facultad de efectuar la mencionada solicitud, se refiere a un marco que se ubica dentro un proceso fiscalizador. Remarcó que la expresión: “Para tales efectos”, reafirma ese concepto.

Consideró que la entrega de cualquier documento, libro o antecedente, debe circunscribirse solo a la fiscalización, y dentro de un proceso de investigación.

El asesor del Ministerio de Hacienda, señor Godoy sugirió la siguiente redacción:

“b) Fiscalizar y velar por el cumplimiento de los principios, derechos y obligaciones establecidos en esta ley. **Para efectos de fiscalización** se podrá solicitar la entrega de cualquier documento, libro o antecedente que sea necesario.”.

Puesta en votación la letra b) del artículo 31, con la enmienda señalada, fue aprobada con el voto favorable de los Honorables Senadores señores De Urresti y Harboe. Se abstuvo el Honorable Senador señor Moreira.

Seguidamente, **el Presidente de la Comisión, Honorable Senador señor Harboe**, sometió a debate la letra c) del artículo 31. Su texto es el siguiente:

“c) Resolver las solicitudes y reclamaciones que formulen los titulares en contra de los responsables de datos.”

El asesor del Comité Udi, señor Mery, observó que la redacción da a entender que se refiere únicamente a las solicitudes de reclamación en contra de los responsables de datos.

Sostuvo que un responsable de datos podrá realizar consultas sobre la aplicación de la ley. Preguntó si esto último está comprendido en la letra en estudio.

El asesor del Ministerio de Hacienda, señor Godoy precisó que la letra c) se refiere solo a las reclamaciones de los titulares.

Aseveró que los responsables de datos pueden solicitar a la autoridad un pronunciamiento específico. Aquello está consagrado dentro de las facultades del Director de la Agencia, específicamente en la letra e) del artículo 33.

Puesta en votación la letra c) del artículo 31, fue aprobada con el voto favorable de los Honorables Senadores señores De Urresti y Harboe. Se abstuvo el Honorable Senador señor Moreira.

A continuación, **el señor Presidente de la Comisión, Honorable Senador señor Harboe**, sometió a debate la letra d) del artículo 31. Su texto es el siguiente:

“d) Investigar y determinar las infracciones en que incurran los responsables de datos y ejercer, en conformidad a la ley, la potestad sancionatoria. Para tales efectos, podrá citar a declarar, entre otros, al titular, a los representantes legales, administradores, asesores y dependientes del responsable de datos, así como a toda persona que haya tenido participación o conocimiento respecto de algún hecho que sea relevante para resolver un procedimiento sancionatorio. Asimismo, podrá tomar las declaraciones respectivas por otros medios que aseguren su fidelidad.”

Sobre esta disposición, **el asesor del Ministerio de Hacienda, señor Godoy,** manifestó que estamos ante una facultad genérica que corresponde normalmente a los organismos que cumplen labores de fiscalización. Ésta consiste en investigar y determinar aquellos hechos que constituyen una infracción a la ley. Agregó que se le otorgan a la Agencia facultades necesarias para cumplir las labores de investigación.

El asesor del Honorable Senador Larraín, señor Olmedo preguntó si se considera una unidad especial dentro de la Agencia, para poder ejercer las facultades de investigación.

Consultó cómo se concilia la tutela de derechos con la posibilidad de llegar a acuerdo entre un reclamante y un infractor.

El asesor del Ministerio de Hacienda, señor Godoy expresó que la iniciativa en estudio establece, en sede administrativa, dos tipos de procedimiento. El primero se inicia cuando un titular de datos ejerce alguno de los derechos que establece la ley y se rechaza dicha solicitud por el responsable de datos. En ese caso, el titular posee el derecho de recurrir a la Agencia con la finalidad de que cautele su derecho. Destacó que en dicho contexto, esta última puede adoptar diversas medidas con el objeto de lograr un acuerdo, lo que llevará a que el procedimiento concluya.

Constató que el segundo procedimiento que contempla la ley es el sancionatorio. Éste puede tener distintos orígenes, como aquel en que la Agencia conoce de un reclamo por tutela de derechos, y a partir de éste, se constata que existe una infracción a la Ley de Protección de Datos personales. Una segunda posibilidad consiste en que dicho órgano lleve a cabo una fiscalización, y producto de ella, detecte que hay un incumplimiento.

Enfatizó que respecto al procedimiento sancionatorio, la Agencia carece de facultades de mediación o arbitraje. Agregó que constatada la infracción a la ley, le corresponde al órgano aplicar la sanción establecida.

El Honorable Senador señor Larraín observó que se presenta el problema de un órgano administrativo con facultades jurisdiccionales. Representó que la misma inquietud se planteó respecto al Servicio Nacional del Consumidor.

Remarcó que surgen dudas en cuanto al ámbito propio de un órgano de este tipo, más todavía cuando estamos en presencia de una autoridad que no es autónoma ni descentralizada.

El Presidente de la Comisión, Honorable Senador señor Harboe, hizo presente que revisó la legislación sobre servicios públicos y éstos tienen un conjunto de potestades. Consignó que gran parte de las instituciones que poseen rango fiscalizador, dependientes de la estructura del Gobierno, tales como el Servicio Nacional de Aduanas; las Superintendencias de Salud y de Educación, Servicio de Impuestos Internos, etcétera, tienen un conjunto de facultades que son más amplias que las aprobadas respecto al proyecto de ley que modifica ley N° 19.496, sobre Protección de los Derechos de los Consumidores.

Enfatizó que ninguno de las instituciones nombradas, poseen autonomía constitucional.

El asesor del Honorable Senador Larraín, señor Olmedo afirmó que los órganos mencionados no tienen como función la tutela de derechos fundamentales, sino que generalmente el buen servicio de la Administración o aspectos impositivos.

El Presidente de la Comisión, Honorable Senador señor Harboe hizo presente que si la protección de datos llega a ser considerada como derecho fundamental, la Agencia deberá contar con mayores facultades que las instituciones mencionadas.

Puesta en votación la letra d) del artículo 31, fue aprobada con el voto favorable de los Honorables Senadores, señores Harboe y Quinteros. Se pronunció en contra el Honorable Senador señor Larraín.

A continuación, **el señor Presidente de la Comisión**, sometió a discusión la letra e) del artículo 31, que dispone lo siguiente:

“e) Adoptar las medidas preventivas o correctivas que disponga la ley.”.

Puesta en votación la letra e) del artículo 31, fue aprobada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Larraín y Quinteros.

Luego, **el señor Presidente de la Comisión**, sometió a debate la letra f) del artículo 31. Su texto es el siguiente:

“f) Proponer al Presidente de la República, por intermedio del Ministerio de Hacienda, las normas legales y reglamentarias para asegurar a las personas la debida protección de sus datos personales y perfeccionar la regulación sobre el tratamiento y uso de esta información.”

Al iniciarse su estudio, **el asesor del Ministerio de Hacienda, señor Godoy,** recordó que a esta Agencia que se le está otorgando autonomía legal, situación que se expresa en dos materias centrales, a saber:

- Es un organismo público descentralizado con personalidad jurídica y patrimonio propio;

- Está sujeto a la supervigilancia del Presidente de la República.

Recalcó que se optó porque la Agencia esté bajo la supervigilancia del Presidente de la República, a través del Ministerio de Hacienda. Ello no significa que esté bajo la tutela del Ministro respectivo. Subrayó que todas las decisiones que adopte la institución son completamente autónomas y solo están sujetas al control jurisdiccional.

Aseveró que lo anterior corresponde a la misma situación jurídica que ocupa la figura de la Fiscalía Nacional Económica.

Agregó que los criterios de autonomía que establece nuestra legislación dicen relación con los sistemas de nombramiento de las autoridades y de su remoción. Constató que el nombramiento es de responsabilidad de la Máxima Autoridad del país y se realiza mediante el sistema de la Alta Dirección Pública. Sostuvo que el período de duración en el cargo es de 5 años, para alejarlo del ciclo político.

En relación a la remoción, consignó que solo se puede pedir por las causales que establece la ley.

El Honorable Senador señor Larraín valoró el esfuerzo realizado por el Ejecutivo, respecto al planteamiento original. Consultó por qué si queremos crear un órgano autónomo, lo constituimos al alero del Ministerio de Hacienda.

Lo anterior, argumentó, puede provocar que el Ministro de Hacienda no haga llegar al Presidente, las propuestas normativas de la Agencia.

El asesor del Comité Udi, señor Mery consideró que con la redacción de la letra en estudio, el Ministro puede rehusarse a comunicar al Presidente la propuesta de la Agencia, por no estar de acuerdo con ella.

Sugirió eliminar la frase: “por intermedio del Ministerio de Hacienda”. Ello puede facilitar la labor del órgano que se está creando.

El asesor del Honorable Senador Larraín, señor Olmedo complementó lo señalado, mencionando que la atribución que se le confiere a la Agencia, de poder presentar al Presidente de la República propuestas de reformas legislativas o reglamentarias es de la más alta trascendencia.

Recordó que en la ley N° 20.405, que crea el Instituto Nacional de Derechos Humanos, se prescribe que éste debe rendir una cuenta anual y presentar un informe al país con presencia del Presidente

de la República. Propuso que se podría exigir algo similar respecto al órgano que se está creando en el cuerpo normativo en estudio.

El asesor del Ministerio de Hacienda, señor Godoy precisó que en el ánimo de fortalecer la autonomía técnica y otorgarle una mayor robustez institucional a la Agencia, el Ejecutivo no advierte dificultades para que se suprima la frase: “por intermedio del Ministerio de Hacienda”.

Hizo presente que lo relevante es que este organismo no tenga la facultad de presentar proyectos al Congreso Nacional, sino que esté sometido a la supervigilancia del Presidente de la República.

Puesta en votación la letra f), del artículo 31, fue aprobada, con la enmienda antes mencionada, por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Larraín y Quinteros.

En seguida, **el señor Presidente de la Comisión**, sometió a votación la letra g) del mencionado artículo 31. Su texto es el siguiente:

“g) Relacionarse con los organismos públicos y con los demás órganos del Estado, en el marco de sus funciones y competencias legales.”

Puesta en votación la letra g), del artículo 31, fue aprobada por la unanimidad de miembros presentes de la Comisión, Honorables Senadores señores Harboe, Larraín y Quinteros.

A continuación, la Comisión examinó la letra h) del artículo 31. Su texto es el siguiente:

“h) Desarrollar programas, proyectos y acciones de difusión, educación, promoción e información dirigidos a la ciudadanía y a los responsables de datos, en relación al respeto y protección del derecho a la vida privada y a la protección de los datos personales.”.

Puesta en votación la letra h), del artículo 31, fue aprobada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Larraín y Quinteros.

Luego, **el señor Presidente de la Comisión** puso en discusión la letra i) del artículo 31. Su texto es el siguiente:

“i) Prestar asistencia técnica, cuando le sea requerida, al Congreso Nacional, al Poder Judicial, a la Contraloría General

de la República, al Ministerio Público, al Tribunal Constitucional, al Banco Central, al Servicio Electoral, a la Justicia Electoral y los demás tribunales especiales creados por ley, para la dictación y ejecución de las políticas y normas internas de estos organismos sobre el tratamiento y la protección de los datos personales.”.

Al iniciarse su análisis, el **asesor del Comité Udi, señor Mery,** manifestó que la asistencia técnica debe prestarse solo cuando sea requerida, y no considerar a ésta como una opinión preferente.

El Presidente de la Comisión, Honorable Senador señor Harboe, resaltó que evidentemente se refiere a asistencia para el cumplimiento de fines al interior de sus instituciones. Subrayó que distinto es que en el marco de un procedimiento judicial se pida la opinión de la Agencia.

El Honorable Senador señor Larraín dejó constancia de que quien desempeña actualmente estas funciones es el Consejo para la Transparencia, por lo que de aprobarse la letra en estudio implicaría modificar el estatuto de dicho Consejo.

El Presidente de la Comisión, Honorable Senador señor Harboe aseveró que el Consejo cumple esa función, porque en la práctica no hay ninguna institución distinta que se haga cargo de ello.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena afirmó que el artículo 33, letra m), de la ley N° 20.285, sobre acceso a la información pública, dispone:

“m) 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.”.

Expresó que para hacer coherente este nuevo organismo y su mandato, en la presente iniciativa se propondrá más adelante la supresión de dicho precepto.

Puesta en votación la letra i), fue aprobada por la mayoría de los miembros presentes de la Comisión, Honorables Senadores señores Harboe y Quinteros. Se pronunció en contra el Honorable Senador señor Larraín.

A continuación, la Comisión consideró la letra j) del artículo 31. Su texto es el siguiente:

“j) Colaborar con los órganos públicos en el diseño e implementación de políticas, programas y acciones destinadas a velar por la protección de los datos personales y su correcto tratamiento.”

Puesta en votación esta letra, fue aprobada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Larraín y Quinteros.

Seguidamente, **el señor Presidente de la Comisión** puso en debate la letra K), del mencionado artículo 31. Su texto es el siguiente:

“k) Celebrar convenios o memorandos de entendimiento con organismos nacionales, internacionales o extranjeros, sean estos públicos o privados y desarrollar programas de asistencia técnica.”.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Harboe, Larraín y Quinteros, aprobó esta letra.

Con la misma votación aprobó la letra l) del artículo 31, disposición que establece que la Agencia podrá participar, recibir cooperación y colaborar con organismos internacionales en materias propias de su competencia.

Seguidamente, **el señor Presidente de la Comisión** sometió a consideración la letra m) del artículo 31. Esta letra dispone lo siguiente:

“m) Solicitar la representación judicial de sus intereses al Consejo de Defensa del Estado de conformidad a la ley.”.

Sobre este precepto, **el asesor del Honorable Senador Larraín, señor Olmedo,** sostuvo que la intervención del Consejo de Defensa del Estado en procedimientos de reclamación, que eventualmente se interpongan en contra de las decisiones de la Agencia, puede generar una afectación a la igualdad procesal, respecto al sector privado. Consideró que la Agencia debiese tener su propio sistema de defensa judicial, puesto que el mencionado Consejo está dotado de atribuciones específicas para velar por los intereses del Fisco.

El asesor del Ministerio de Hacienda, señor Godoy consignó que no comparte que se produzca una afectación al principio de la igualdad procesal entre las partes, en virtud de la representación del Consejo de Defensa del Estado.

Añadió que este último tiene diversas facultades de representación de los intereses del Estado, y en el caso planteado consistiría en asumir la representación de una institución nueva.

La razón de haber ocupado la fórmula que se sugiere, es que la Agencia que se crea es eminentemente técnica, sin capacidad de absorber la defensa judicial. Constató que el órgano se situará en la Región Metropolitana y carecerá del despliegue territorial. Por lo tanto, como la función de representación judicial de sus intereses debe ser desarrollado a lo largo del país, se optó porque la defensa jurídica de ella, se realice a través del Consejo de Defensa del Estado.

Finalmente, recordó que existen varias instituciones que son representadas judicialmente por dicho Consejo.

El Honorable Senador señor Larraín solicitó que el señor Godoy profundice su última afirmación.

El asesor del Ministerio de Hacienda, señor Godoy ejemplificó con la Comisión del Mercado Financiero, entidad que se encuentra en la misma situación de la Agencia.

Agregó que cuando un decreto que proviene de los Ministerios y las Subsecretarías, es rechazado, el Consejo es el encargado de asumir la representación de los mencionados organismos.

El Honorable Senador señor Larraín sugirió la siguiente redacción:

m) Asumir o solicitar al Consejo de Defensa del Estado, en conformidad a la ley, la representación judicial de sus intereses.

El asesor del Comité Udi, señor Mery expuso que la Agencia podrá actuar por sí misma o contratar servicios profesionales para gestiones específicas. Hizo presente que la letra en estudio explicita la facultad que posee todo organismo público, a saber, acudir al Consejo de Defensa del Estado.

Puesta en votación la letra m), con la enmienda propuesta, fue aprobada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Larraín y Quinteros.

Enseguida, se examinó la letra n) del artículo 31. Su texto es el siguiente:

“n) Certificar, registrar y supervisar los modelos de prevención de infracciones y los programas de cumplimiento y administrar el Registro Nacional de Cumplimiento y Sanciones.”.

Sobre esta disposición, **el asesor del Ministerio de Hacienda, señor Godoy,** destacó que se le otorga a la Agencia la facultad de certificar y mantener el Registro Nacional de Cumplimientos y Sanciones.

Consignó que una de las mayores innovaciones que tiene la presente iniciativa, consiste en promover los modelos de auto cumplimiento de la ley. Agregó que los responsables de datos pueden asumir voluntariamente instrumentos que permiten regular un cumplimiento efectivo de la ley al interior de sus propias organizaciones.

Manifestó que como los mencionados modelos son relativamente nuevos en nuestra legislación, es útil que la Agencia adopte, en esta primera etapa, una función activa. Detalló que en muchas jurisdicciones la certificación de este tipo de modelo está entregada a las agencias privadas.

En relación al Registro de Responsables de Datos, relató que la norma que hoy existe en la ley N° 19.628, se refiere a aquellas bases de datos que poseen los órganos públicos. Éstos tienen la obligación de inscribirlas en el Registro Civil.

Opinó que dicho Registro carece de utilidad y se encuentra desactualizado. Constató que lo anterior es distinto a avanzar hacia un Registro de Responsables de Datos del sector público y privado.

Destacó que las legislaciones modernas en materia de protección de datos han ido desarrollando un modelo en que las empresas deben comunicar en sus páginas web un conjunto de información que permita que los titulares puedan saber cuáles son las bases de datos; cuáles son los tipos de tratamientos de datos que realizan, etcétera.

El Presidente de la Comisión, Honorable Senador señor Harboe expresó que la existencia de un gobierno corporativo y de los mecanismos de prevención responden a una tendencia de la legislación moderna.

Puesta en votación esta letra, fue aprobada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Larraín y Quinteros.

A continuación, la Comisión examinó la letra o) del artículo 31. Esta disposición establece lo siguiente:

“ñ) Resolver las solicitudes y controversias que se susciten sobre si una determinada base de datos o conjunto de datos es considerada fuente de acceso público e identificar categorías genéricas, clases o tipos de datos, conjuntos de datos o bases de datos que posean esta condición.”.

Al iniciarse su estudio, **el Honorable Senador señor Larraín** consultó por el tipo de controversias que resolverá la Agencia.

El Presidente de la Comisión, Honorable Senador señor Harboe contestó que se refiere a aquellas en que surjan dudas acerca de si una determinada base de datos es de acceso público o no.

El Honorable Senador señor Larraín preguntó en qué instancia se produce la actuación de la Agencia.

El abogado analista del Consejo para la Transparencia, señor Alejandro González, estimó que el punto en discusión es fundamental respecto a las competencias que posee el Consejo, en relación al concepto de fuentes de acceso público.

Opinó que las controversias que se van a suscitar pueden constituir un flanco que puede llegar a judicializarse. Agregó que al entregar esta competencia, desde el punto de vista administrativo, a la Agencia, se pierde el punto de equilibrio entre las competencias de ambos órganos respecto al concepto de fuente de acceso público, fundamental para resolver eventuales controversias. Por eso, es primordial acotarlo.

El Presidente de la Comisión, Honorable Senador señor Harboe propuso que se reemplace la expresión “controversias”, por “consultas”.

El asesor del Ministerio de Hacienda, señor Godoy reconoció que el término “consulta” es más apropiado.

El Honorable Senador señor Larraín sugirió la siguiente redacción:

“ñ) Resolver las solicitudes o consultas relativas a si una determinada base de datos o conjunto de datos es considerada fuente de acceso público e identificar categorías genéricas que posean esta condición.”.

Puesta en votación la letra ñ), con la enmienda señalada, fue aprobada por la unanimidad de los miembros presentes

de la Comisión, Honorables Senadores señores Harboe, Larraín y Quinteros.

Luego, el señor Presidente de la Comisión, puso en discusión la letra o) del artículo 31. Su texto es el siguiente:

“o) Ejercer las demás funciones y atribuciones que la ley le encomiende.”.

Puesta en votación esta letra fue aprobada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Harboe, Larraín y Quinteros.

El texto acordado precedentemente fue ratificado mediante una indicación que presentó el Ejecutivo, la que se dio por aprobada con las votaciones señaladas precedentemente.

Artículo 32

A continuación, la Comisión examinó el nuevo artículo 32 que incorpora el proyecto de ley del Ejecutivo a la ley N° 19.628. En esta disposición se regula el tema de la coordinación regulatoria. Su texto es el siguiente:

“Artículo 32.- Coordinación regulatoria. Cuando la Agencia de Protección de Datos Personales deba dictar una instrucción o norma de carácter general y obligatoria que pueda tener efectos en los ámbitos de competencia del Consejo para la Transparencia, de acuerdo a las funciones y atribuciones señaladas en la ley N° 20.285, le remitirá todos los antecedentes y requerirá de éste un informe para efectos de evitar o precaver conflictos de normas y asegurar la coordinación, cooperación y colaboración entre ambos órganos.

El Consejo para la Transparencia deberá evacuar el informe solicitado dentro del plazo de treinta días corridos, contado desde la fecha en que hubiere recibido el requerimiento a que se refiere el inciso precedente.

La Agencia de Protección de Datos Personales considerará el contenido de la opinión del Consejo para la Transparencia expresándolo en la motivación de la instrucción o norma que dicte, de conformidad a lo dispuesto en el artículo 41 de la ley N° 19.880. Transcurrido el plazo sin que se hubiere recibido el informe, se procederá conforme al inciso segundo del artículo 38 de dicha ley.

A su vez, cuando el Consejo para la Transparencia deba dictar una instrucción general que tenga claros efectos en los ámbitos de competencia de la Agencia de Protección de Datos Personales, de acuerdo a las funciones y atribuciones señaladas en esta ley, el Consejo remitirá los antecedentes y requerirá informe a la Agencia de Protección de Datos Personales, quien deberá evacuarlo en el plazo de treinta días corridos, contado desde la fecha en que hubiere recibido el requerimiento. El Consejo considerará el contenido de la opinión de la Agencia de Protección de Datos Personales expresándolo en la motivación de la instrucción general que dicte al efecto.”.

Al iniciarse el estudio de esta disposición, los representantes del Ejecutivo propusieron a la Comisión aprobar esta norma, enmendada en los siguientes términos:

“Artículo 32.- Coordinación regulatoria. Cuando la Agencia de Protección de Datos Personales deba dictar **una instrucción general** que pueda tener efectos en los ámbitos de competencia del Consejo para la Transparencia, de acuerdo a las funciones y atribuciones señaladas en la ley N° 20.285, le remitirá todos los antecedentes y requerirá de éste un informe para efectos de evitar o precaver conflictos de normas y asegurar la coordinación, cooperación y colaboración entre ambos órganos.

El Consejo para la Transparencia deberá evacuar el informe solicitado dentro del plazo de treinta días corridos, contado desde la fecha en que hubiere recibido el requerimiento a que se refiere el inciso precedente.

La Agencia de Protección de Datos Personales valorará el contenido de la opinión del Consejo para la Transparencia expresándolo en la motivación de la instrucción que dicte, de conformidad a lo dispuesto en el artículo 41 de la ley N° 19.880. Transcurrido el plazo sin que se hubiere recibido el informe, se procederá conforme al inciso segundo del artículo 38 de **esa** misma ley.

A su vez, cuando el Consejo para la Transparencia deba dictar una instrucción general que tenga claros efectos en los ámbitos de competencia de la Agencia de Protección de Datos Personales, de acuerdo a las funciones y atribuciones señaladas en esta ley, el Consejo remitirá los antecedentes y requerirá informe a la Agencia de Protección de Datos Personales, quien deberá evacuarlo en el plazo de treinta días corridos, contado desde la fecha en que hubiere recibido el requerimiento. El Consejo valorará el contenido de la opinión de la Agencia de Protección de Datos Personales expresándolo en la motivación de la instrucción general que dicte al efecto.

Cuando la instrucción general afecte a cualquier otro órgano de la Administración del Estado, se aplicará lo dispuesto en el artículo 37 bis de la ley N° 19.880.”.

Al iniciarse el estudio de este precepto, **la asesora del Ministerio de Economía, señora Bernardita Piedrabuena,** sostuvo que este artículo responde a una modificación realizada recientemente con motivo de la aprobación de la ley N° 21.000, que crea la Comisión para el Mercado Financiero. En ese cuerpo legal se llevó a cabo una alteración al artículo 37 bis de la ley N° 19.880. En el mencionado artículo se habla de coordinación regulatoria entre las agencias del Estado.

Expresó que dicha norma había que reiterarla en la presente iniciativa, dado que al Consejo no se le aplica la ley N° 19.880.

El Honorable Senador señor Larraín reiteró que es recomendable que en una sola entidad se reúnan las funciones de protección de datos y de transparencia.

Constató que estamos ante dos instituciones con naturalezas jurídicas diversas. Por un lado el Consejo para la Transparencia que está dotado de autonomía y en cuya designación participan distintos órganos del Estado. Por el otro, la Agencia de Protección de Datos que cuenta con un Director administrativo, dentro de un Ministerio. Aseveró que, desde el punto de vista de la naturaleza administrativa, se produce, entre ambas, un desnivel jerárquico. Agregó que ninguno de los órganos resulta obligado respecto del otro.

El Presidente de la Comisión, Honorable Senador señor Harboe, recordó que la Agencia será un órgano independiente, y distinto del Consejo. Consideró que el riesgo de entregarle al Consejo ambas facultades, implicaría que el acceso a la información pública se vea debilitado por la masividad de consultas, reclamos y controversias en materia de protección de datos personales.

Estimó que es probable que exista una diferencia entre ambas instituciones y no solo respecto a la jerarquía, sino que también en cuanto a sus funciones y en la naturaleza jurídica.

Observó que el Director de la Agencia no será un director administrativo dentro de un Ministerio. Remarcó que el sistema de nombramiento genera una interrelación con diferentes poderes del Estado y las causales de remoción están establecidas por ley. Indicó que se ha avanzado, en la práctica, en un nivel de mayor autonomía, tanto orgánico como decisional. Añadió que las decisiones que adopte la Agencia no son revisables por la autoridad gubernativa, solo por una autoridad jurisdiccional.

Destacó que la norma en estudio obligará a ambos órganos a coordinarse y generará una forma de coordinación.

El asesor del Ministerio de Hacienda, señor Godoy, advirtió que el Consejo para la Transparencia no tiene mayor jerarquía que la Agencia de Protección de Datos. Precisó que la jerarquía de un organismo en nuestro sistema no está dada porque un órgano sea colegiado o unipersonal.

Señaló que ambas instituciones son servicios públicos descentralizados, que están bajo la supervigilancia del Presidente de la República. Por tanto, desde el punto de vista jerárquico, tienen el mismo nivel.

El asesor del Honorable Senador Larraín, señor Olmedo, preguntó si se le está otorgando al Poder Judicial la decisión regulatoria en función de instrucciones.

Consignó que lo que puede ocurrir, es que frente a opiniones diversas de una y otra institución, un tercero podrá recurrir a los tribunales de justicia. Afirmó que con ello, la facultad de instrucción va estar entregada al Poder Judicial.

Sugirió profundizar en un mecanismo que permita evadir la judicialización de la facultad mencionada.

El asesor del Comité Udi, señor Mery, sostuvo que cuando se trata de la resolución de un conflicto de esta clase, se resuelve un acto determinado. Cuando el Poder Judicial resuelve una controversia aclara si éste es o no legal. No surge la potestad, para este Poder, de generar una norma de carácter general.

Llamó la atención la diferente redacción entre el inciso primero y cuarto. El primero de ellos dispone: “Cuando la Agencia de Protección de Datos Personales deba dictar una instrucción general que pueda tener efectos en los ámbitos de competencia del Consejo para la Transparencia…”. Por su parte, el inciso cuarto prescribe: “A su vez, cuando el Consejo para la Transparencia deba dictar una instrucción general que tenga claros efectos en los ámbitos de competencia de la Agencia de Protección de Datos Personales…”.

Consultó si existe una razón para aquella redacción.

Precisó que si se quiere decir lo mismo, debieran unificarse las expresiones, para evitar confusiones futuras.

El Presidente de la Comisión, Honorable Senador señor Harboe, manifestó que la ley N° 19.880, que establece las bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado, es de carácter general. Agregó que diversos fallos del Tribunal Constitucional han señalado que corresponde a un cuerpo normativo que se aplica a todos los órganos del Estado.

Expuso que el artículo 32 en estudio está en concordancia con el artículo 38 de la ley N° 19.880, que establece el valor de los informes cuando se trata de autoridades públicas.

Respecto a lo señalado por el asesor, señor Olmedo, recordó que en la práctica son los tribunales de justicia los que terminan resolviendo cuestiones relacionadas con las materias en estudio. Expresó que lo anterior se está tratando de evitar mediante esta iniciativa de ley.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena, reconoció que son constantes los recursos que se interponen ante los tribunales de justicia. Añadió que ellos no solo se circunscriben al tema de acceso a la transparencia versus protección de datos.

El Honorable Senador señor Larraín insistió que el Consejo para la Transparencia y la Agencia no tendrán la misma naturaleza jerárquica, por la forma en que están constituidos, y por la designación de sus integrantes. Estimó que la diferencia obra en favor del mencionado Consejo.

Opinó que lo deseable es que la labor de protección de datos quede bajo el alero del Consejo para la Transparencia. En subsidio de ello, es partidario de que se genere una institución completamente autónoma.

Puesto en votación el artículo 32, fue aprobado en los términos propuestos por el Ejecutivo, por mayoría de votos. Votaron a favor los Honorables Senadores señores Harboe y Quinteros Se abstuvo el Honorable Senador señor Larraín.

El texto acordado precedentemente fue ratificado mediante una indicación que presentó el Ejecutivo, la que se dio por aprobada con las votaciones señaladas precedentemente.

Artículo 33

A continuación, la Comisión consideró el artículo 33 que el proyecto de ley del Ejecutivo, disposición que agrega a la ley N° 19.628 las normas relativas a la dirección de la Agencia de Protección de Datos. Su texto es el siguiente:

"Artículo 33.- Del Director o Directora de la Agencia de Protección de Datos Personales. La dirección y administración superior de la Agencia de Protección de Datos Personales estará a cargo de un Director o Directora, quien será el jefe superior del Servicio, nombrado por el Presidente de la República conforme al Sistema de Alta Dirección Pública regulado en el título VI de la ley N° 19.882, afecto al primer nivel jerárquico.

Son funciones y atribuciones del Director o Directora las siguientes:

a) Velar por el respeto, defensa y protección de los derechos y libertades de las personas que son titulares de datos, en particular el derecho a la vida privada, promoviendo una cultura de información, educación y participación ciudadana de acuerdo a los principios y derechos establecidos en esta ley.

b) Fiscalizar y supervigilar el tratamiento de los datos personales que realicen las personas naturales y jurídicas con el objeto que cumplan los principios y obligaciones establecidos en esta ley.

c) Asesorar al Ministro o Ministra de Hacienda en el estudio y proposición de las reformas legales aplicables al tratamiento de los datos personales y su protección.

d) Interpretar administrativamente las disposiciones legales en materia de protección y tratamiento de datos personales, dictar normas generales e impartir instrucciones para su aplicación y fiscalización.

e) Absolver las consultas sobre la aplicación e interpretación de las normas relativas a la protección de datos y su tratamiento que formulen las personas naturales y jurídicas.

f) Planificar las labores de fiscalización de la Agencia de Protección de Datos Personales y desarrollar políticas y programas que promuevan la prevención y la autorregulación.

g) Dirigir, organizar, planificar y coordinar el funcionamiento de la Agencia de Protección de Datos Personales; dictar las

órdenes necesarias para una marcha expedita de ésta y supervigilar el cumplimiento de las instrucciones que imparta.

h) Representar a la Agencia de Protección de Datos Personales en todos los asuntos que le competan, incluidos recursos judiciales y los recursos extraordinarios que se interpongan en contra de la Dirección con motivo de actuaciones administrativas o jurisdiccionales.

i) Presentar al Ministerio de Hacienda, antes del 31 de marzo de cada año, una memoria anual sobre la marcha de la Agencia de Protección de Datos Personales.

j) Proponer al Presidente de la República, por intermedio del Ministerio de Hacienda, las medidas que, a su juicio, convenga adoptar para la mejor marcha de la Agencia de Protección de Datos Personales y desarrollar todas las iniciativas tendientes a tal fin."

Al iniciarse el estudio de esta norma, **los representantes del Ejecutivo, señora Piedrabuena y señor Godoy**, propusieron reordenar este precepto en los siguientes términos:

"Artículo 33.- Del Director o Directora de la Agencia de Protección de Datos Personales. La dirección y administración superior de la Agencia de Protección de Datos Personales estará a cargo de un Director o Directora, quien será el jefe superior del Servicio, nombrado por el Presidente de la República conforme al Sistema de Alta Dirección Pública regulado en el Título VI de la ley N° 19.882, afecto al primer nivel jerárquico.

El Director o Directora de la Agencia de Protección de Datos Personales durará cinco años en su cargo, pudiendo renovarse su nombramiento por una sola vez.

El Director o Directora cesará en sus funciones por las siguientes causales:

a) Término del período legal de su designación.

b) Renuncia voluntaria aceptada por el Presidente de la República.

c) Sobreviniencia de alguna causal de inhabilidad o incompatibilidad.

d) Incapacidad física o síquica para el desempeño del cargo.

e) Incumplimiento grave de sus funciones y deberes.

La remoción por las causales señaladas en las letras d) y e) será dispuesta por el Presidente de la República, con el informe favorable de la Corte Suprema, a requerimiento fundado del Ministro o Ministra de Hacienda. El informe favorable deberá ser emitido por el pleno de la Corte, especialmente convocado al efecto, y deberá reunir el voto conforme de la mayoría de sus miembros en ejercicio.

Sin perjuicio de los requisitos generales para ingresar a la Administración Pública, el Director o Directora deberá ser una persona de reconocido prestigio profesional o académico y acreditar experiencia laboral relevante.

Son funciones y atribuciones del Director o Directora las siguientes:

a) Velar por el respeto, defensa y protección del derecho a la vida privada de las personas en relación al tratamiento de sus datos personales, promoviendo una cultura de información, educación y participación ciudadana de acuerdo a los principios y derechos establecidos en la ley.

b) Dictar las instrucciones, circulares, oficios y resoluciones que se requieran.

c) Asesorar y proponer al Ministro o Ministra de Hacienda, las reformas legales o reglamentarias necesarias en el ámbito de las funciones y competencias de la Agencia de Protección de Datos Personales.

d) Interpretar administrativamente las disposiciones legales en materia de tratamiento y protección de los datos personales e impartir instrucciones para su aplicación y fiscalización.

e) Absolver las consultas sobre la aplicación e interpretación de las normas relativas al tratamiento y protección de los datos personales.

f) Planificar y dirigir las labores de fiscalización de la Agencia de Protección de Datos Personales y desarrollar políticas y programas que promuevan la prevención y la autorregulación.

g) Aplicar las sanciones de conformidad a lo establecido en esta ley y resolver los recursos legales correspondientes.

h) Dirigir, organizar, planificar y coordinar el funcionamiento de la Agencia de Protección de Datos Personales; dictar las órdenes necesarias para una marcha expedita de la misma y supervigilar el cumplimiento de las normas e instrucciones que imparta.

i) Representar a la Agencia de Protección de Datos Personales en todos los asuntos que le competan, incluidos recursos judiciales y los recursos extraordinarios que se interpongan en contra de la Dirección con motivo de actuaciones administrativas o jurisdiccionales.

j) Presentar al Ministerio de Hacienda, antes del 31 de marzo de cada año, una memoria anual sobre la marcha de la Agencia de Protección de Datos Personales.

k) Resolver la celebración de los actos, contratos y convenciones necesarias para el cumplimiento de las funciones de la Agencia.

l) Delegar las atribuciones o facultades derivadas de su calidad de jefe de servicio en funcionarios de la Agencia.

Las demás funciones y atribuciones que le encomiende la ley.”

Sobre esta disposición, **el Honorable Senador señor Larraín** sugirió utilizar la expresión “Director”, en el entendido que esta función puede ser desempeñada tanto por un hombre o por una mujer.

Respecto a la designación del Director, destacó que se requiere de un nombramiento que otorgue plena autonomía al órgano. Propuso que el Senado participe en este proceso.

Por otra parte, objetó la forma de remoción del Director, ya que se le concede al Ministro de Hacienda la atribución de solicitarla, mediante un requerimiento fundado. Ello da cuenta del grado de dependencia que la Agencia posee con el Ministerio de Hacienda.

El Presidente de la Comisión, Honorable Senador señor Harboe hizo presente que es importante que participe otro poder del Estado en el nombramiento, para poder garantizar la autonomía. Coincidió con el Honorable Senador señor Larraín, en cuanto a no incorporar al Ministro de Hacienda en el proceso de remoción.

Consideró relevante establecer un control externo a la institucionalidad que se está creando.

Asimismo, se mostró partidario que el Director permanezca en su cargo por cinco años, para que éste no coincida con el ciclo político.

El Honorable Senador, señor Quinteros abogó por no incorporar al Senado en el proceso de designación del Director. Enfatizó que con el término del sistema binominal, las Cámaras poseerán diversidad de opiniones, lo que podrá llevar a que este tipo de nombramientos se alargue innecesariamente.

Agregó que si se desea incorporar al Senado, deben establecerse en la presente iniciativa, los quórum necesarios que eviten paralizar el nombramiento.

El Honorable Senador señor Larraín recalcó que el fundamento del cambio de sistema electoral no aplica cuando se trata de una autoridad unipersonal. Sostuvo que puede buscarse una fórmula para evitar eventuales efectos paralizantes en el nombramiento. Reiteró que es partidario que el Senado intervenga en la designación del Director.

El Honorable Senador señor Quinteros aseveró que el parlamento iniciará una etapa en que los acuerdos no serán fáciles de alcanzar.

El Presidente de la Comisión, Honorable Senador señor Harboe, afirmó que veto de la minoría constituye un problema.

El asesor del Ministerio de Hacienda, señor Godoy, manifestó que la forma de remoción corresponde al mismo sistema incorporado respecto al Fiscal Nacional Económico, organismo que goza de autonomía legal y prestigio técnico en nuestro sistema jurídico.

Estimó que no existe dificultad de eliminar el informe del Ministro de Hacienda en esta materia.

Desde el punto de vista del nombramiento, señaló que en el artículo 30, que introduce la creación de la Agencia, se define a ésta como un organismo técnico. Reconoció que hacer participar a un órgano esencialmente político, como el Senado, en su nombramiento, significa en algún grado desvirtuar la naturaleza del órgano que se está creando.

Subrayó que resulta más robusto un sistema de nombramiento, mediante concurso público a través del mecanismo de la Alta Dirección Pública.

En cuanto al control externo que pudiese recaer sobre la Agencia, recordó que la acusación constitucional está pensada solo para autoridades políticas.

El Presidente de la Comisión, Honorable Senador señor Harboe, sugirió que el Ejecutivo prepare una propuesta.

Agregó que no comparte el argumento del asesor, señor Godoy, en cuanto a que el carácter técnico del órgano exima la posibilidad de que intervenga el Senado en la designación. Hizo presente que la Cámara Alta participa de nombramientos de autoridades, que no tienen el carácter de políticas, como es en el caso de los Ministros de la Corte Suprema.

El Honorable Senador señor Larraín propuso que la Alta Dirección Pública le entregue una nómina al Presidente de la República, y que la Máxima Autoridad haga participar del nombramiento al Senado, tal como ocurre en la designación de otras autoridades.

Sugirió que dentro del procedimiento de remoción, intervenga la Cámara de Diputados, mediante la solicitud de un número determinado de parlamentarios.

El Presidente de la Comisión, Honorable Senador señor Harboe reiteró que no es partidario que el Ministro de Hacienda participe en la remoción del Director de la Agencia. Insistió que se debe buscar una fórmula diversa.

El asesor del Comité Udi, señor Mery, sugirió que en el inciso tercero del artículo en estudio se modifique la letra c, que dispone: “c) Sobreviniencia de alguna causal de inhabilidad o incompatibilidad.”, por: “c) Sobreviniencia de las causales de inhabilidad o incompatibilidad contempladas en el artículo 34 de esta ley.”.

Se mostró disconforme con que se requiera para la remoción de un informe favorable de la Corte Suprema, ya que una vez que se pronuncia el Máximo Tribunal, deja en absoluta indefensión al Director.

En una sesión posterior, la Comisión continuó con el análisis de la iniciativa, específicamente lo que dice relación con la designación y la remoción del Director de la Agencia.

El asesor del Ministerio de Hacienda, señor Godoy, manifestó que en la perspectiva de fortalecer la autonomía técnica e institucional de la Agencia de Protección de Datos Personales, tanto en

nombramiento como en la remoción del Director, deberían participar dos poderes del Estado.

Respecto al nombramiento, estimó que debe llevarse a cabo mediante un sistema de concurso, a través de la Alta Dirección Pública. Agregó que posterior a ello, le corresponderá al Presidente de la República nominar un candidato, que debe ser ratificado por el Senado, por mayoría simple.

En cuanto a la remoción, remarcó que ésta debe producirse por causales establecidas en la ley, a propuesta del Presidente de la República y contar con la ratificación del Pleno de la Corte Suprema.

Consideró que el Presidente de la República tiene que estar presente en ambas instancias, porque la Agencia es un órgano que pertenece a la Administración del Estado.

El Honorable Senador señor Larraín se mostró conforme con la propuesta del Ejecutivo, ya que ésta acerca posiciones. Insistió en que la Agencia debe ser autónoma, y ello se ha ido logrando durante la discusión del presente proyecto.

Se mostró contrario con el quórum de mayoría simple, porque constituye una exigencia para quien gobierne. Connotó que en el sistema proporcional imperante, la mayoría absoluta constituye una garantía para todos, porque obliga alcanzar acuerdos.

El Honorable Senador señor Araya sostuvo que es partidario del quórum simple. Agregó que el nombramiento está resguardado por el sistema que se propone.

Manifestó sus dudas respecto al proceso de remoción. Estimó que no hay que cerrar la posibilidad de que ésta pueda ser solicitada por la Cámara de Diputados.

El Honorable Senador señor Larraín recordó que el artículo 89 de nuestra Carta Fundamental prescribe:

“El Fiscal Nacional y los fiscales regionales sólo podrán ser removidos por la Corte Suprema, a requerimiento del Presidente de la República, de la Cámara de Diputados, o de diez de sus miembros, por incapacidad, mal comportamiento o negligencia manifiesta en el ejercicio de sus funciones….”

De acuerdo a lo anterior, propuso que la Cámara Baja pueda participar en la destitución del Director de la Agencia.

El Presidente de la Comisión, Honorable Senador señor Harboe precisó que es deseable que el Senado participe en el nombramiento y la Cámara de Diputados en la remoción.

El asesor del Ministerio de Hacienda, señor Godoy destacó que en cuanto a la remoción no incluiría a la Cámara Baja, porque eventualmente, si el Presidente de la República se niega a la destitución del Director, se puede generar un conflicto entre ambos poderes del Estado.

El Honorable Senador señor Larraín consignó que el Director de la Agencia no es una autoridad política, sino que se le está confiriendo una cierta garantía de autonomía.

Recalcó que debe reproducirse el artículo 38 de la ley N° 20.285, sobre acceso a la información pública, que en su inciso primero señala:

“Artículo 38.- Los consejeros serán removidos por la Corte Suprema, a requerimiento del Presidente de la República, de la Cámara de Diputados mediante acuerdo adoptado por simple mayoría, o a petición de diez diputados, por incapacidad, mal comportamiento o negligencia manifiesta en el ejercicio de sus funciones. La Corte Suprema conocerá del asunto en pleno especialmente convocado al efecto y para acordar la remoción deberá reunir el voto conforme de la mayoría de sus miembros en ejercicio.”.

Insistió que exigir mayoría absoluta del Senado en su nombramiento le confiere mayor fuerza al Director.

El Presidente de la Comisión, Honorable Senador señor Harboe estimó que con el objetivo de otorgarle la misma jerarquía al Consejo para la Transparencia y a la Agencia de Protección de Datos, es una buena solución la propuesta de incorporar al Senado en la designación y a la Cámara de Diputados en la destitución del Director.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena aseveró que si en la designación participa el Senado, debe fijarse un plazo prudente para ello.

En relación a la remoción, sugirió que ésta pueda originarse por la mayoría simple de sus integrantes.

A continuación, el asesor del Honorable Senador Larraín, señor Olmedo, consultó si se debiese exigir el título de abogado para desempeñar el cargo de Director. Añadió que para efectos de

ampliar el escenario de posibles candidatos, podría también exigirse experiencia en la protección el derecho a la privacidad.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena manifestó que la experiencia requerida debe recaer sobre la protección de datos. Expresó que el Director de la Agencia puede ser un abogado o un ingeniero.

Indicó que se debe tener precaución cuando se establecen ciertas restricciones, tal como la de acreditar años de experiencia. Consignó que es el sistema de la Alta Dirección Pública el llamado a exigir dicho requisito. Destacó que ello puede desalentar a las mujeres, que poco a poco se han ido insertando en el mercado laboral.

El Honorable Senador señor Larraín compartió que son tres los requisitos que deben cumplirse para ser Director de la Agencia, a saber: Prestigio profesional o académico; experiencia laboral relevante en la materia y algunos años de ejercicio profesional. Sostuvo que lo recomendable es a lo menos 10 años de ejercicio de la profesión.

La Honorable Senadora señora Allende expresó que resulta complejo acreditar experiencia laboral relevante si estamos ante una materia reciente.

El Presidente de la Comisión, Honorable Senador señor Harboe, connotó que el Director debe contar con un título profesional acorde a la materia. Respecto a la experiencia profesional, recordó que la ley N° 19.628, sobre protección de la vida privada, fue publicada el año 1999. Por lo tanto, existen profesionales que llevan un tiempo considerable dedicado a la mencionada materia.

Declaró que la exigencia de 10 años de ejercicio profesional puede significar que ciertas profesionales mujeres no cumplan con ese requisito. Enfatizó que tanto el título profesional, como la experiencia laboral, deben estar relacionados con la protección de datos.

El asesor del Ministerio de Hacienda, señor Godoy, aseveró que la experiencia laboral relevante, debe recaer en las funciones y competencias de la Agencia. Consideró que podría exigirse 7 años de ejercicio profesional.

La Honorable Senadora señora Allende se mostró partidaria de requerir 5 años.

El Presidente de la Comisión, Honorable Senador señor Harboe apuntó que el Director ejercerá potestades muy relevantes, tanto fiscalizadoras, como normativas y sancionadoras. Por lo

tanto, es recomendable exigir 5 años de ejercicio profesional, relacionado con la materia de la protección de datos.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena declaró que debe ponderarse el requisito de 5 años de experiencia en la materia. Destacó que lo relevante lo constituye la idoneidad del candidato.

El Honorable Senador señor Larraín aseveró que puede ser útil lo ocurrido en el Consejo para la Transparencia. Subrayó que en dicha institución ha habido profesionales de distinta historia, quizás sin tanta experiencia, que han logrado un buen trabajo.

Acotó que debiesen ser distintas las exigencias para el primer Director de la Agencia. Relató que en la elección del primero, no exigiría antigüedad. Estimó razonable que para los Directores siguientes se exija 10 años de experiencia profesional en el área.

En una sesión posterior, la Comisión debatió la siguiente redacción para el artículo 33. Ella surgió de una propuesta que formularon **los representantes del Ejecutivo, señora Piedrabuena y señor Godoy**. Su texto es el siguiente:

Artículo 33.- Del Director de la Agencia de Protección de Datos Personales. La dirección y administración superior de la Agencia de Protección de Datos Personales estará a cargo de un Director, quien será el jefe superior del Servicio, nombrado por el Presidente de la República conforme al Sistema de Alta Dirección Pública regulado en el Título VI de la ley N° 19.882, afecto al primer nivel jerárquico.

El nombramiento efectuado por el Presidente de la República será ratificado por el Senado, en sesión especialmente convocada al afecto, por la mayoría simple de sus miembros. El Presidente de la República deberá proponer al Senado el nombramiento 60 días antes de la expiración del plazo de duración del Director saliente. El Senado dispondrá de un plazo de 30 días para aceptar o rechazar la propuesta. En caso que no se pronuncie dentro de este plazo, se entenderá aceptada la proposición del Presidente de la República. Este procedimiento se repetirá tantas veces fuere necesario, hasta obtener la aprobación por el Senado a la proposición que formule el Presidente de la República. Otorgada esa aprobación, el Presidente de la República, por intermedio del Ministerio de Hacienda, expedirá el decreto supremo de nombramiento del Director de la Agencia de Protección de Datos Personales.

El Director de la Agencia de Protección de Datos Personales durará cinco años en su cargo, pudiendo renovarse su nombramiento por una sola vez.

El Director cesará en sus funciones por las siguientes causales:

a) Término del período legal de su designación.

b) Renuncia voluntaria aceptada por el Presidente de la República.

c) Sobreviniencia de alguna causal de inhabilidad o incompatibilidad establecida en el artículo 34.

d) Incapacidad física o síquica para el desempeño del cargo.

e) Incumplimiento grave de sus funciones y deberes.

La remoción por las causales señaladas en las letras d) y e) será dispuesta por la Corte Suprema a requerimiento del Presidente de la República o de la Cámara de Diputados mediante acuerdo adoptado por simple mayoría. La Corte Suprema conocerá del asunto en pleno especialmente convocado al efecto y para acordar la remoción deberá reunir el voto conforme de la mayoría de sus miembros en ejercicio.

Para ser nombrado Director de la Agencia de Protección de Datos Personales, se requiere:

i. Cumplir con los requisitos generales para ingresar a la Administración Pública;

ii. Tener a lo menos siete años de ejercicio profesional;

iii. Contar con reconocido prestigio profesional o académico en el ámbito de la protección de los datos personales, y

iv. Acreditar experiencia laboral relevante en materias relacionadas con las funciones y competencias de la Agencia de Protección de Datos Personales.

Al iniciarse el estudio de esta disposición, el asesor del Ministerio de Hacienda, señor Godoy, explicó que en ella se han excluido las menciones a las funciones y atribuciones del Director de la Agencia, las que se considerarán en un artículo 33 bis, nuevo, que se analizará más adelante.

Sobre esta nueva propuesta, **el Honorable Senador señor Larraín** valoró que se considere la participación del Senado en la designación de esta autoridad. Sin embargo, insistió que el quórum para aprobar al candidato debiera ser mayoría absoluta.

El asesor del Ministerio de Hacienda, señor Godoy, estimó que la mayoría simple es suficiente para efectos del nombramiento del Director de la Agencia.

El Honorable Senador señor Larraín enfatizó que se busca que la Agencia adquiera un grado de consenso importante y con un respaldo que supere las mayorías circunstanciales. Consignó que para lograr lo anterior, se requiere un quórum más alto a la mayoría simple.

El Honorable Senador, señor Araya suscribió lo expresado por el Honorable Senador señor Larraín.

Como una forma de llegar a un consenso en esta materia, **el señor Presidente de la Comisión** informó que el Ejecutivo había presentado una nueva indicación para sustituir este precepto. Su texto es el siguiente:

"Artículo 33.- Del Director o Directora de la Agencia de Protección de Datos Personales. La dirección y administración superior de la Agencia de Protección de Datos Personales estará a cargo de un Director, quien será el jefe superior del Servicio.

Será designado por el Presidente de la República, conforme al Sistema de Alta Dirección Pública regulado en el título VI de la ley N° 19.882, afecto al primer nivel jerárquico, y con acuerdo del Senado adoptado por la mayoría absoluta de sus miembros en ejercicio.

El Presidente de la República deberá proponer esta designación sesenta días antes de la expiración del plazo de duración del Director saliente. El Senado dispondrá de un término de treinta días corridos para aceptar o rechazar la propuesta. En caso que no se pronuncie dentro de este plazo se entenderá aceptada la proposición del Presidente de la República. Si el Senado rechaza la proposición del Presidente de la República se deberá repetir el procedimiento hasta que se apruebe o acepte una designación. Otorgada esa aprobación o aceptación, según corresponda, el Presidente de la República, por intermedio del Ministerio de Hacienda, expedirá el decreto supremo de nombramiento del Director o Directora de la Agencia de Protección de Datos Personales.

El Director o Directora de la Agencia de Protección de Datos Personales durará cinco años en su cargo, pudiendo renovarse su nombramiento por una sola vez.

El Director cesará en sus funciones por las siguientes causales:

a) Término del período legal de su designación.

b) Renuncia voluntaria aceptada por el Presidente de la República.

c) Sobreviniencia de alguna causal de inhabilidad o incompatibilidad establecida en el artículo 34.

d) Incapacidad física o síquica para el desempeño del cargo.

e) Incumplimiento grave de sus funciones y deberes.

La remoción por las causales señaladas en las letras d) y e) será dispuesta por la Corte Suprema a requerimiento del Presidente de la República o de la Cámara de Diputados mediante acuerdo adoptado por simple mayoría. La Corte Suprema conocerá del asunto en pleno especialmente convocado al efecto y para acordar la remoción deberá reunir el voto conforme de la mayoría de sus miembros en ejercicio.

Para ser nombrado Director o Directora de la Agencia de Protección de Datos Personales, se requiere:

i. Cumplir con los requisitos generales para ingresar a la Administración Pública;

ii. Tener a lo menos siete años de ejercicio profesional;

iii. Contar con reconocido prestigio profesional o académico en el ámbito de la protección de los datos personales, y

iv. Acreditar experiencia laboral relevante en materias relacionadas con las funciones y competencias de la Agencia de Protección de Datos Personales.”.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, De Urresti, Harboe y Larraín, aprobó este precepto con la única enmienda de

suprimir las menciones a “Ministra” y “Directora” que aparece en su texto, confirmando un decisión que sobre la materia se adoptó al aprobar el artículo 14 sexies.

Artículo 33 bis

En una sesión posterior, **los representantes del Ejecutivo, señora Piedrabuena y señor Godoy**, propusieron a la Comisión aprobar un artículo 33 bis, nuevo, que regula las funciones atribuciones del Director de la Agencia. Su texto es el siguiente:

“Artículo 33 bis.- De las funciones y atribuciones del Director. Son funciones y atribuciones del Director las siguientes:

a) Velar por el respeto, defensa y protección del derecho a la vida privada de las personas en relación al tratamiento de sus datos personales, promoviendo una cultura de información y educación en esta materia, de acuerdo a los principios y derechos establecidos en la ley.

b) Promover la participación ciudadana en las materias relacionadas con la protección y el tratamiento de los datos personales, de acuerdo a los principios y derechos establecidos en la ley.

c) Dictar las instrucciones, circulares, oficios y resoluciones que se requieran.

d) Proponer al Presidente de la República las reformas legales o reglamentarias necesarias en el ámbito de las funciones y competencias de la Agencia de Protección de Datos Personales.

e) Interpretar administrativamente las disposiciones legales en materia de tratamiento y protección de los datos personales e impartir instrucciones para su aplicación y fiscalización.

f) Absolver las consultas sobre la aplicación e interpretación de las normas relativas al tratamiento y protección de los datos personales.

g) Planificar y dirigir las labores de fiscalización de la Agencia de Protección de Datos Personales y desarrollar políticas y programas que promuevan la prevención y la autorregulación.

h) Aplicar las sanciones de conformidad a lo establecido en esta ley y resolver los recursos legales correspondientes.

i) Dirigir, organizar, planificar y coordinar el funcionamiento de la Agencia de Protección de Datos Personales; dictar las órdenes necesarias para una marcha expedita de la misma y supervigilar el cumplimiento de las normas e instrucciones que imparta.

j) Representar a la Agencia de Protección de Datos Personales en todos los asuntos que le competan, incluidos recursos judiciales y los recursos extraordinarios que se interpongan en contra de la Dirección con motivo de actuaciones administrativas o jurisdiccionales, en coordinación con el Consejo de Defensa del Estado, según corresponda.

k) Presentar al Presidente de la República, antes del 31 de marzo de cada año, una memoria anual sobre la marcha de la Agencia de Protección de Datos Personales y dar cuenta pública de ella.

l) Resolver la celebración de los actos, contratos y convenciones necesarias para el cumplimiento de las funciones de la Agencia.

m) Delegar sus funciones y atribuciones en funcionarios de su dependencia, de conformidad a la ley.

n) Las demás funciones y atribuciones que le encomiende la ley.

Al explicar esta propuesta, **el asesor del Ministerio de Hacienda, señor Godoy,** indicó que la mayoría de las letras ya estaban consideradas en el artículo 33 del Mensaje del Ejecutivo. Agregó que la letra a) original, se dividió en dos letras, ya que estimó que la defensa y protección del derecho a la vida privada y la promoción de la participación ciudadana, constituían funciones distintas del Director.

El asesor del Honorable Senador Larraín, señor Olmedo, consultó el significado de la frase: “en coordinación con el Consejo de Defensa del Estado.”, que figura en la letra j) de este artículo.

El asesor del Ministerio de Hacienda, señor Godoy expresó que la representación judicial de la Agencia le corresponde a su Director. Sin embargo, consignó que se pueden promover litigios a lo largo del país, y en esos casos, la Agencia podrá recurrir al Consejo de Defensa del Estado.

Seguidamente, **el asesor del Ministerio de Hacienda, señor Godoy**, señaló que, además, en esta nueva propuesta se simplificó la redacción de la letra m) para precisar la delegación de funciones.

El Presidente de la Comisión, Honorable Senador señor Harboe, recordó que la delegación funciones no genera delegación de responsabilidades.

Concluido el análisis de esta disposición, el señor Presidente de la Comisión, la sometió a votación.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, De Urresti y Harboe, aprobó el artículo 33 bis.

El texto acordado precedentemente fue ratificado mediante una indicación que presentó el Ejecutivo, la que se dio por aprobada con las votaciones señaladas precedentemente.

Artículo 34

En seguida, el proyecto de ley del Ejecutivo, propone agregar un artículo 34 a la ley N° 19.628. Esta disposición prescribe lo siguiente:

“Artículo 34.- Incompatibilidades e Inhabilidades. El desempeño del cargo de Director o Directora exige dedicación exclusiva y es incompatible con el desempeño de todo otro cargo o servicio, sea o no remunerado, que se preste en el sector privado. Asimismo, este cargo es incompatible con todo otro empleo o servicio retribuido con fondos fiscales o municipales, y con las funciones, remuneradas o no, de consejero, director o trabajador de instituciones públicas, organismos autónomos nacionales o extranjeros, empresas del Estado y, en general, de todo servicio público creado por ley, como, asimismo, de empresas, sociedades o entidades públicas o privadas en que el Estado, sus empresas, sociedades o instituciones centralizadas o descentralizadas, tengan aportes de capital mayoritario o en igual proporción o en las mismas condiciones, representación o participación. También es incompatible con cualquier otro servicio o empleo remunerado o gratuito en otros poderes del Estado.

El cargo de Director o Directora es compatible con el desempeño de cargos docentes en instituciones públicas o privadas reconocidas por el Estado, hasta un máximo de doce horas semanales. Del mismo modo, el Director o Directora puede desempeñarse en corporaciones o fundaciones, públicas o privadas, nacionales o extranjeras, siempre que en ellas no perciba remuneración y su desempeño no sea incompatible con sus funciones.

Él o la cónyuge o conviviente civil del Director o Directora y sus parientes hasta el segundo grado de consanguinidad

inclusive, no podrán ser director o directora ni tener participación en la propiedad de una empresa cuyo objeto o giro comercial verse sobre recolección, tratamiento o comunicación de datos personales.

En todo lo no expresamente regulado en este artículo, regirán las normas del párrafo 2 del título III de la ley Nº 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado, cuyo texto refundido, coordinado y sistematizado fue fijado por el decreto con fuerza de ley N° 1-19653, de 2000, del Ministerio Secretaría General de la Presidencia.”

Al iniciarse el estudio de este precepto, **los representantes del Ejecutivo, señora Piedrabuena y señor Godoy,** sugirieron a la Comisión aprobar el texto del proyecto de ley del Gobierno, enmendado en los siguientes términos:

“Artículo 34.- Incompatibilidades e Inhabilidades. El desempeño del cargo de Director o Directora exige dedicación exclusiva y es incompatible con el desempeño de todo otro cargo o servicio, sea o no remunerado, que se preste en el sector privado. Asimismo, este cargo es incompatible con todo otro empleo o servicio retribuido con fondos fiscales o municipales, y con las funciones, remuneradas o no, de consejero, director o trabajador de instituciones públicas, organismos autónomos nacionales o extranjeros, empresas del Estado y, en general, de todo servicio público creado por ley, como, asimismo, de empresas, sociedades o entidades públicas o privadas en que el Estado, sus empresas, sociedades o instituciones centralizadas o descentralizadas, tengan aportes de capital mayoritario o en igual proporción o, en las mismas condiciones, representación o participación. También es incompatible con cualquier otro servicio o empleo remunerado o gratuito en otros poderes del Estado.

El cargo de Director o Directora es compatible con el desempeño de cargos docentes en instituciones públicas o privadas reconocidas por el Estado, hasta un máximo de doce horas semanales. Del mismo modo, el Director o Directora puede desempeñarse en corporaciones o fundaciones, públicas o privadas, nacionales o extranjeras, siempre que en ellas no perciba remuneración y su desempeño no sea incompatible con sus funciones.

Él o la cónyuge o conviviente civil del Director o Directora y sus parientes hasta el segundo grado de consanguinidad inclusive, no podrán ser director o directora ni tener participación en la propiedad de una empresa cuyo objeto o giro comercial verse sobre recolección, tratamiento o comunicación de datos personales.

No podrá ser designado Director o Directora:

1. La persona que hubiere sido condenada por delito que merezca pena aflictiva o inhabilitación perpetua para desempeñar cargos u oficios públicos, por delitos de prevaricación, cohecho y, en general, aquellos cometidos en ejercicio de la función pública, delitos tributarios y los delitos contra la fe pública.

2. La persona que tuviere dependencia de sustancias o drogas estupefacientes o sicotrópicas cuya venta no se encuentre autorizada por la ley, a menos que justifique su consumo por un tratamiento médico.

3. La persona que esté siendo objeto de un procedimiento sancionatorio o que haya sido sancionada, dentro de los últimos tres años, por infracción gravísima a las normas que regulan el tratamiento de los datos personales y su protección.

En todo lo no expresamente regulado en este artículo, regirán las normas del párrafo 2° del Título III de la ley Nº 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado.”.

Respecto al inciso primero, **el Presidente de la Comisión, Honorable Senador señor Harboe** observó que este precepto hace incompatible el cargo de Director con el desempeño del cargo de consejero, director o trabajador de instituciones extranjeras. Preguntó si este cargo de es incompatible con el de integrar un Comité de Protección de Datos a nivel internacional.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena, precisó que en el inciso segundo se permite que el Director pueda desempeñarse en corporaciones o fundaciones, públicas o privadas, nacionales o extranjeras, siempre que en ellas no perciba remuneración y su desempeño no sea incompatible con sus funciones.

El Honorable Senador señor Larraín consultó si la remuneración que percibirá la mencionada autoridad, es compatible con las restricciones que se consagran.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena manifestó que la remuneración corresponderá al primer nivel jerárquico de la Administración Pública.

El asesor del Ministerio de Hacienda, señor Godoy, detalló que en el artículo séptimo transitorio se señala el grado asignado al Director, que corresponde al 1C, de la Escala Única de Sueldos.

Agregó que la única actividad remunerada adicional que puede desarrollar el Director, corresponde al desempeño de cargos docentes en instituciones públicas o privadas reconocidas por el Estado, hasta un máximo de doce horas semanales.

Puesto en votación el inciso primero del artículo 34, fue aprobado por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Araya, Harboe y Larraín.

En seguida se examinó el inciso segundo de esta disposición que establece lo siguiente:

“El cargo de Director o Directora es compatible con el desempeño de cargos docentes en instituciones públicas o privadas reconocidas por el Estado, hasta un máximo de doce horas semanales. Del mismo modo, el Director o Directora puede desempeñarse en corporaciones o fundaciones, públicas o privadas, nacionales o extranjeras, siempre que en ellas no perciba remuneración y su desempeño no sea incompatible con sus funciones.”.

El Honorable Senador señor Larraín sugirió utilizar el término “asociación”, debido a su amplitud.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena connotó que los diferentes jefes de servicio, como el de la Unidad de Análisis Financiero y los de algunas Superintendencias, sí participan de asociaciones extranjeras. Lo anterior se encuentra permitido, ya que ellos lo hacen como representantes de los servicios cuya jefatura ejercen.

El Presidente de la Comisión, Honorable Senador señor Harboe recordó que el Director puede ejercer funciones en organismos internacionales, siempre que éstas no sean remuneradas.

El Honorable Senador señor Larraín afirmó que dentro de las funciones del Director, no se encuentra la de representar a la Agencia ante organismos internacionales. Insistió en la necesidad que se incorpore el término “asociaciones” al inciso en estudio.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena aseveró que la mencionada función está contemplada en el artículo 31, letra l), que señala:

“l) Participar, recibir cooperación y colaborar con organismos internacionales en materias propias de su competencia.”.

El asesor del Ministerio de Hacienda, señor Godoy sugirió la siguiente redacción para solucionar lo planteado:

“Del mismo modo, el Director puede desempeñarse en organismos o asociaciones, públicas o privadas, nacionales o extranjeras, siempre que en ellas no perciba remuneración y su desempeño no sea incompatible con sus funciones.”.

Puesto en votación el inciso segundo, con la enmienda señalada, fue aprobado por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Araya, Harboe y Larraín.

Con la misma votación se aprobó el inciso tercero.

En seguida, se examinó el inciso cuarto, disposición que establece lo siguiente:

“No podrá ser designado Director o Directora:

1. La persona que hubiere sido condenada por delito que merezca pena aflictiva o inhabilitación perpetua para desempeñar cargos u oficios públicos, por delitos de prevaricación, cohecho y, en general, aquellos cometidos en ejercicio de la función pública, delitos tributarios y los delitos contra la fe pública.”

El Presidente de la Comisión, Honorable Senador señor Harboe remarcó que se inhabilita a aquellas personas que han sido condenadas por determinados delitos. Preguntó si no serán considerados como causal de inhabilidad aquellos delitos que no han sido cometidos en el ejercicio de la función pública, que afecten la fe pública y la probidad.

Advirtió que el cohecho corresponde a un tipo penal propio de privados. Sugirió se modifique la redacción.

Consultó si puede ser Director de la Agencia quien ha sido condenado por el delito de quiebra fraudulenta, o por haber infringido gravemente la protección de datos personales.

El asesor del Ministerio de Hacienda, señor Godoy, expresó que la norma indica que cualquier delito que merezca pena aflictiva, independiente de cuál sea, imposibilita que una persona postule al cargo de Director.

Sugirió eliminar la expresión “en general”, ya que ella genera confusión. Aseveró que se consideran, dentro de la hipótesis planteada, los delitos funcionarios; los tributarios y aquellos que afectan la fe pública.

Precisó que en el número 3, se consagra la inhabilidad para la persona que esté siendo objeto de un procedimiento sancionatorio o que haya sido sancionada, dentro de los últimos tres años, por infracción gravísima a las normas que regulan el tratamiento de los datos personales y su protección.

Puesto en votación el numeral 1, con la enmienda señalada, fue aprobado por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Araya, Harboe y Larraín.

En seguida, se puso en discusión el número 2, disposición que establece lo siguiente:

“2. La persona que tuviere dependencia de sustancias o drogas estupefacientes o sicotrópicas cuya venta no se encuentre autorizada por la ley, a menos que justifique su consumo por un tratamiento médico.”.

El asesor del Ministerio de Hacienda, señor Godoy apuntó que en diversos cuerpos normativos de los organismos fiscalizadores se ha ido avanzando, en términos de ser más estrictos al momento de fijar incompatibilidades e inhabilidades. Agregó que una de ellas está constituida por la dependencia a las sustancias o drogas antes mencionadas.

El Honorable Senador señor Araya compartió lo señalado por el señor asesor. Sin embargo, estimó que existe una contradicción en la norma, puesto que si la sustancia se encuentra prohibida, un médico no podría justificar su uso, salvo en el caso de la marihuana.

Sugirió eliminar la frase: “, a menos que justifique su consumo por un tratamiento médico.”.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena ratificó que las sustancias psicotrópicas que pueden ser recetadas por un médico, deben ser legales.

El asesor del Comité Udi, señor Mery, propuso revisar la Ley Orgánica Constitucional de Bases Generales de la Administración del Estado, ya que en ella puede encontrarse una solución a lo observado.

En una sesión posterior, los mencionados representantes del Ejecutivo propusieron la siguiente redacción alternativa:

"2. La persona que tuviere dependencia de sustancias o drogas estupefacientes o sicotrópicas ilegales, a menos que justifique su consumo por un tratamiento médico.".

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, De Urresti y Harboe, aprobó este número del artículo 34.

En seguida se analizó el número 3 de esta disposición. Su texto es el siguiente:

"3. La persona que esté siendo objeto de un procedimiento sancionatorio o que haya sido sancionada, dentro de los últimos tres años, por infracción gravísima a las normas que regulan el tratamiento de los datos personales y su protección."

El Presidente de la Comisión, Honorable Senador señor Harboe, manifestó que alguien que ha sido denunciado por infracción, goza del principio de inocencia. Por lo tanto, la inhabilidad debe recaer sobre quien ha sido sancionado por estos hechos.

Sugirió la siguiente redacción:

"3. La persona que haya sido sancionada, dentro de los últimos tres años, por infracción gravísima a las normas que regulan el tratamiento de los datos personales y su protección."

El Honorable Senador señor Larraín propuso que el que postula al cargo no sea militante de un partido político.

El Presidente de la Comisión, Honorable Senador señor Harboe se mostró contrario a esta idea, porque implica inmiscuirse en la vida privada del candidato al cargo. Constató que la adscripción política constituye un dato sensible.

Puesto en votación el número 3, con la enmienda señalada, fue aprobado por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Araya, Harboe y Larraín.

Por último se consideró el inciso final de este precepto que dispone lo siguiente:

“En todo lo no expresamente regulado en este artículo, regirán las normas del párrafo 2° del Título III de la ley Nº 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado.”

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó esta disposición.

El texto acordado precedentemente fue ratificado mediante una indicación que presentó el Ejecutivo, la que se dio por aprobada con las votaciones señaladas precedentemente.

Artículo 35

A continuación, la Comisión examinó el artículo 35 del proyecto de ley del Ejecutivo. Esta disposición regula el régimen de personal de los trabajadores de la Agencia de Protección de Datos Personales. Su texto es el siguiente:

“Artículo 35.- Del personal. El personal de la Agencia de Protección de Datos Personales estará afecto a las disposiciones de la ley N° 18.834, sobre Estatuto Administrativo, cuyo texto refundido, coordinado y sistematizado fue fijado por el decreto con fuerza de ley N° 29, de 2004, y en materia de remuneraciones, a las normas del decreto ley N° 249, de 1974, que fija Escala Única de Sueldos, y su legislación complementaria.

En caso de ejercerse acciones judiciales por actos formales, acciones u omisiones producidos en el ejercicio de su cargo, en contra del personal de la Agencia de Protección de Datos Personales, incluido su Director o Directora, la Agencia de Protección de Datos Personales deberá proporcionarles defensa jurídica. Esta defensa se extenderá a todas aquellas acciones que se inicien en su contra por los motivos señalados, incluso después de haber cesado en el cargo.”.

En relación a esta proposición, **los representantes del Ejecutivo** sugirieron a la Comisión aprobar el texto del Ejecutivo, enmendado en los siguientes términos:

“Artículo 35.- Del personal. El personal de la Agencia de Protección de Datos Personales estará afecto a las disposiciones del decreto con fuerza de ley N° 29, de 2004, que fija el texto refundido, coordinado y sistematizado de la ley N° 18.834, sobre Estatuto Administrativo y, en materia de remuneraciones, a las normas del decreto ley N° 249, de 1974, que fija Escala Única de Sueldos, y su legislación complementaria.

En caso de ejercerse acciones judiciales por actos formales, acciones u omisiones producidos en el ejercicio de su cargo, en contra del personal de la Agencia de Protección de Datos Personales, incluido su Director o Directora, la Agencia de Protección de Datos Personales deberá proporcionarles defensa jurídica. Esta defensa se extenderá a todas aquellas acciones que se inicien en su contra por los motivos señalados, incluso después de haber cesado en el cargo.”.

En relación al primer inciso, **el Presidente de la Comisión, Honorable Senador señor Harboe** sugirió simplificar su redacción.

Para ello, propuso el siguiente texto:

“Artículo 35.- Del personal. El personal de la Agencia de Protección de Datos Personales estará afecto al Estatuto Administrativo y, en materia de remuneraciones, a la Escala Única de Sueldos.”.

El Honorable Senador señor Larraín preguntó si el personal que forme parte de la Agencia celebrará un contrato de trabajo. Lo anterior, para evitar la rigidez del órgano que se está creando.

El asesor del Honorable Senador Larraín, señor Olmedo, recordó que fue clave en la instalación del Consejo para la Transparencia la flexibilidad laboral que entrega el contrato de trabajo.

El asesor del Ministerio de Hacienda, señor Godoy, aseveró que cuando se planteó la necesidad del Ejecutivo de crear la Agencia, se pensó en un servicio público descentralizado, que forme parte de la Administración del Estado.

Desde esa perspectiva, observó que el régimen jurídico que se debe seguir es el del estatuto administrativo.

Constató que desde el punto de vista de los grados de flexibilidad que tiene el futuro Director para la gestión del personal, solo los cargos de carácter directivo formarán parte de la planta del órgano. Agregó que las demás personas que formen parte de la Agencia, estarán bajo la modalidad del contrato de trabajo.

El asesor del Ministerio de Hacienda, señor Godoy, subrayó que todos ellos formarán parte de la Escala Única de Sueldos. Añadió que por una parte están los funcionarios de Planta, y por el otro, aquellos cuya contratación se autoriza por ley. Estos últimos son

funcionarios públicos sujetos al estatuto administrativo, que no se encuentran dentro de la Planta. Por lo tanto, no tienen la condición de ser inamovibles.

El Honorable Senador señor Larraín acotó que si se desea flexibilizar el Estado, no se deben crear organismos cargados de burocracia, ya que eso dificulta su funcionamiento.

El asesor del Ministerio de Hacienda, señor Godoy, remarcó que a la Comisión de Constitución, Legislación, Justicia y Reglamento le correspondió discutir la Ley que fortalece el Ministerio Público. En el mencionado cuerpo legal se estableció un modelo de carrera funcionaria, pero sujeto al Código del Trabajo.

El Presidente de la Comisión, Honorable Senador señor Harboe manifestó que no es el momento de dar la discusión. Sin embargo, observó que actualmente en el Estado se ha producido un estancamiento en la carrera funcionaria y una falta de eficacia y eficiencia. Connotó que las autoridades han tenido que duplicar las dotaciones con personal a honorarios para suplir las deficiencias de personal de planta.

El asesor del Comité Udi, señor Mery, señaló que se debe precisar que se refiere a acciones judiciales interpuestas por terceros.

El Presidente de la Comisión, Honorable Senador señor Harboe propuso que la redacción de la norma excluya aquellos casos en los que se denuncie a un funcionario de la Agencia por violación de secreto.

En todo caso, **el Honorable Senador señor Larraín** dejó constancia que se está perdiendo una oportunidad para dotar a un organismo del Estado de una estructura más ágil y menos burocrática.

En una sesión posterior, **el asesor del Ministerio de Hacienda, señor Godoy,** presentó una indicación del Ejecutivo para consignar este precepto en los siguientes términos:

Artículo 35.- Del personal. El personal de la Agencia de Protección de Datos Personales estará afecto al decreto con fuerza de ley N° 29, de 2004, del Ministerio de Hacienda que fija el texto refundido, coordinado y sistematizado de la ley N° 18.834 sobre Estatuto Administrativo y, en materia de remuneraciones, a las normas del decreto ley N° 249, de 1974, y su legislación complementaria.

En caso que terceros ejerzan en contra del personal de la Agencia de Protección de Datos Personales, incluido su Director, acciones judiciales por actos formales o por acciones u omisiones

producidas en el ejercicio de sus cargos, la Agencia de Protección de Datos Personales deberá proporcionarles defensa jurídica. Esta defensa se extenderá a todas aquellas acciones que se inicien en su contra incluso después de haber cesado en el cargo.

No procederá la defensa a que se refiere el inciso anterior en los casos en que los actos formales, acciones u omisiones en cuestión hayan configurado una causal de cesación imputable a la conducta del respectivo funcionario.”.

El asesor del Ministerio de Hacienda, señor Godoy explicó que respecto a los funcionarios públicos existen tres tipos de estatutos administrativos. A saber, el de los funcionarios de la Administración centralizada; el de los funcionarios municipales y el que se aplica a los que trabajan en la atención primaria. Enfatizó que, atendido lo anterior, debe especificarse el estatuto que se aplica a los funcionarios de la Agencia de Protección de Datos Personales.

Luego de un breve intercambio de opiniones, **el señor Presidente de la Comisión** sometió a votación este precepto haciendo presente que esta es una materia que corresponde la iniciativa exclusiva del Ejecutivo.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, De Urresti Harboe y Larraín, aprobó esta disposición.

Finalmente, **el Presidente de la Comisión, Honorable Senador señor Harboe,** concordó con la idea de modernizar al Estado. Ello implica buscar, por ejemplo, mecanismos de contratación que consideren las normas del Código del Trabajo.

Hizo presente que cada vez que se crean organismos públicos, la inamovilidad atenta en contra del buen funcionamiento de los servicios públicos. Constató que la creación de nuevas instituciones debiera contar con un régimen laboral bastante más moderno que el actual.

Artículo 36

A continuación, la Comisión se abocó al estudio del artículo 36 que propone el proyecto de ley del Ejecutivo. En esta disposición se regula el tema del patrimonio de la Agencia de Protección de Datos Personales. Su texto es el siguiente:

“Artículo 36.- Del patrimonio. El patrimonio de la Agencia de Protección de Datos Personales estará formado por:

a) El aporte que se contemple anualmente en la Ley de Presupuestos de la Nación.

b) Los bienes muebles e inmuebles que se le transfieran o que adquieran a cualquier título y por los frutos que de ellos se perciban.

c) Las donaciones que la Agencia de Protección de Datos Personales acepte. Las donaciones no requerirán del trámite de insinuación judicial a que se refiere el artículo 1401 del Código Civil.

d) Las herencias y legados que la Agencia de Protección de Datos Personales acepte, lo que deberá hacer siempre con beneficio de inventario. Dichas asignaciones estarán exentas de toda clase de impuestos y de todo gravamen o pago que les afecten.

e) Los aportes de la cooperación internacional.”.

Al iniciarse el estudio de este precepto, **el Presidente de la Comisión, Honorable Senador señor Harboe**, se mostró partidario de que un porcentaje de las multas que se apliquen se destinen a la Agencia. Lo anterior con el objetivo de crear un órgano con capacidad efectiva y que pueda llevar a cabo un buen trabajo.

El Honorable Senador señor Larraín agregó que debe consagrarse una cláusula abierta que permita a la Agencia incorporar otras fuentes de financiamiento.

El asesor del Ministerio de Hacienda, señor Godoy sostuvo que recientemente se aprobó una experiencia en la reforma laboral, en que las multas por infracción a los derechos colectivos del trabajo iban a un fondo destinado a programas de capacitación de actores sociales. Expresó que para lograr ese objetivo, fue necesario crear un fondo especial con una cierta institucionalidad, denominado Consejo Superior Laboral. Este último es el llamado a tomar decisiones respecto a la gestión de dicho fondo. Consideró que para la mayoría de los servicios se genera un incentivo para cobrar multas.

El asesor del Comité Udi, señor Mery, sostuvo que existen buenas razones para pensar en una idea como la planteada, porque ella está asociada a la eficiencia y al desempeño correcto de las funciones. Sin embargo, advirtió que pueden originarse incentivos perversos y de esa manera desnaturalizarse la función del Servicio.

Apuntó que puede idearse un mecanismo para evitar este último tipo de incentivos.

Puesto en votación el artículo 36, fue aprobado por la unanimidad de los Honorables Senadores presentes señores Araya, Harboe y Larraín.

En una sesión posterior, el Ejecutivo propuso agregar una letra f), nueva a este precepto.

En él se dispone lo siguiente:

“f) Los demás aportes o recursos que se le otorguen por ley.”.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, De Urresti y Harboe, aprobó esta materia.

El texto acordado precedentemente fue ratificado mediante una indicación que presentó el Ejecutivo, la que se dio por aprobada con las votaciones señaladas precedentemente.

Artículo 37

Seguidamente, la Comisión analizó el artículo 37 del proyecto de ley del Ejecutivo, con el que se da inicio al nuevo Título VII de la ley N° 19.628: Este Título establece las reglas aplicables a las infracciones de esta ley y sus sanciones, así como a los procedimientos y obligaciones de los responsables de datos. El texto de este precepto es el siguiente:

“Artículo 37.- Régimen general de responsabilidad. El responsable de datos, sea una persona natural o jurídica, de derecho público o privado, que en sus operaciones de tratamiento de datos personales infrinja los principios y obligaciones establecidos en esta ley, será sancionado de conformidad con las normas del presente título.”.

Puesto en votación este precepto, fue aprobado por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Araya, Harboe y Larraín.

Artículo 38

A continuación, la Comisión trató el artículo 38 del proyecto de ley del Ejecutivo. En esta disposición se establecen los distintos tipos de infracciones que pueden cometer quienes vulneren los deberes o las obligaciones que se establece este proyecto de ley. Su texto es el siguiente:

"Artículo 38.- Infracciones leves, graves y gravísimas. Las infracciones a los principios y obligaciones establecidos en esta ley cometidas por los responsables de datos se califican, atendida su gravedad, en leves, graves y gravísimas.

Se consideran infracciones leves las siguientes:

a) El incumplimiento total o parcial del deber de información y transparencia.

b) No disponer de una dirección de correo electrónico o de un medio electrónico equivalente, actualizado y operativo, a través del cual los titulares de datos puedan dirigir sus comunicaciones o ejercer sus derechos.

c) No responder o responder fuera de plazo las solicitudes formuladas por el titular de datos en conformidad a esta ley.

d) No informar o no remitir a la Agencia de Protección de Datos Personales las comunicaciones previstas en esta ley o en sus reglamentos.

e) No dar cumplimiento a las instrucciones impartidas por la Agencia de Protección de Datos Personales que no estén sancionadas específicamente como infracción grave o gravísima.

f) No efectuar el bloqueo temporal de los datos personales del titular cuando éste lo haya solicitado fundadamente o denegar la solicitud sin causa justificada.

g) Impedir el ejercicio legítimo del derecho a la portabilidad de los datos personales del titular.

h) Cometer cualquier otra infracción a los principios, deberes y obligaciones establecidas en esta ley que no sea calificada como una infracción grave o gravísima.

Se consideran infracciones graves las siguientes:

a) Tratar los datos personales sin contar con el consentimiento previo del titular de datos o sin la habilitación legal correspondiente o tratarlos con una finalidad distinta de aquélla para la cual fueron recolectados.

b) Comunicar o ceder datos personales sin el consentimiento del titular o cederlos para un fin distinto del autorizado por el titular.

c) Vulnerar en las operaciones de tratamiento de datos que realice, en forma manifiesta, los principios de proporcionalidad, calidad, seguridad y responsabilidad.

d) Realizar tratamiento de datos personales sensibles y de datos personales de niños, niñas y adolescentes con infracción a las normas previstas en esta ley.

e) Realizar tratamiento de datos personales sin cumplir los requisitos establecidos para las fundaciones, asociaciones o cualquier otra entidad que no persiga fines de lucro y cuya finalidad sea política, filosófica, religiosa, cultural, deportiva, sindical o gremial, respecto de los datos de sus asociados.

f) Vulnerar el deber de secreto o confidencialidad establecido en el artículo 14 bis.

g) Impedir u obstaculizar el ejercicio legítimo de los derechos de acceso, rectificación, cancelación u oposición del titular.

h) No adoptar las medidas de seguridad que resulten adecuadas, necesarias y oportunas para el tratamiento de datos y que se encuentren previstas en esta ley, en el reglamento respectivo o en las instrucciones de la Agencia de Protección de Datos Personales.

i) No efectuar las comunicaciones o no realizar los registros correspondientes en los casos de vulneración de las medidas de seguridad, según lo establecido en el artículo 14 quinquies.

j) Realizar operaciones de transferencia internacional de datos en contravención a las normas previstas en esta ley.

k) Adoptar medidas de calidad y seguridad insuficientes o no idóneas para el tratamiento de datos personales con fines históricos, estadísticos o científicos y para estudios o investigaciones que atiendan fines de interés público.

l) Entregar información falsa, incompleta o manifiestamente errónea en el proceso de registro o certificación del modelo de prevención de infracciones.

m) Recolectar maliciosamente a través de niños, niñas o adolescentes datos personales de integrantes de su grupo familiar.

n) No dar cumplimiento a las instrucciones específicas y directas que le haya impartido la Agencia de Protección de Datos Personales.

Se consideran infracciones gravísimas las siguientes:

a) Efectuar tratamiento de datos personales de manera manifiestamente fraudulenta.

b) Destinar maliciosamente los datos personales a una finalidad distinta de la consentida por el titular o prevista en la ley que autoriza su tratamiento.

c) Comunicar, transmitir o ceder a terceros, a sabiendas, información no veraz, incompleta, inexacta o desactualizada del titular de datos.

d) Vulnerar, a sabiendas, el deber de secreto o confidencialidad sobre los datos personales sensibles y datos personales relativos a la comisión y sanción de infracciones penales, civiles, administrativas y disciplinarias.

e) Comunicar o ceder a terceros, a sabiendas, datos personales sensibles sin el consentimiento del titular y en contravención a las normas dispuestas en el párrafo segundo del título II de esta ley.

f) Tratar datos personales sensibles con manifiesta falta de diligencia o cuidado.

g) No comunicar oportunamente, habiendo estado en conocimiento de ello y disponiendo de los medios para hacerlo, la vulneración de la medidas de seguridad que puedan afectar la confidencialidad, disponibilidad o integridad de los datos personales.

h) Actuar con falta de diligencia o cuidado en la protección de los datos personales que conciernen a los niños, niñas y adolescentes, especialmente respecto de quienes pesa la obligación especial de cuidado de esta información y que con ocasión de ello, se han efectuado

tratamientos de datos de niños, niñas y adolescentes con infracción a las normas de esta ley.”

Al iniciarse el estudio de esta materia, se tuvo presente que la moción parlamentaria que se refunde en este proyecto también contiene normas relativas a las infracciones a la ley. Esta materia aparece regulada en los artículos 37 y 38 de la mencionada moción. Su texto es el siguiente:

“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.

Al iniciarse el estudio de estas proposiciones, **los representantes del Ejecutivo, señora Piedrabuena y señor Godoy**, sugirieron a la Comisión aprobar el proyecto de ley del Ejecutivo, enmendado en los siguientes términos:

“Párrafo Primero

De la responsabilidad, las infracciones y las sanciones aplicables a las personas naturales o jurídicas de derecho privado

Artículo 38.- Infracciones leves, graves y gravísimas. Las infracciones cometidas por los responsables de datos a los principios, derechos y obligaciones establecidos en esta ley se califican, atendida su gravedad, en leves, graves y gravísimas.

Las responsabilidades en que incurra una persona natural o jurídica por las infracciones establecidas en esta ley, se entienden sin perjuicio de las demás responsabilidades legales, civiles o penales, que pudieran corresponderle.”

Al explicar esta proposición, **el abogado asesor del Ministerio de Hacienda, señor Godoy,** señaló que se había decidido regular específicamente los distintos tipos de infracciones, en los artículos 38 bis, 38 ter y 38 quáter, materias que originalmente estaban consideradas en el artículo 38.

Dada esta explicación, **el Presidente de la Comisión, Honorable Senador señor Harboe**, puso en votación el artículo 38 del proyecto de ley del Ejecutivo, enmendado en los términos indicados precedentemente.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó esta disposición.

El texto acordado precedentemente fue ratificado mediante una indicación que presentó el Ejecutivo, la que se dio por aprobada con la votación señalada precedentemente.

Artículo 38 bis

A continuación, la Comisión consideró el artículo 38 bis, propuesto por los representantes del Ejecutivo. En esta disposición se regula las conductas que se consideran infracciones leves. Su texto es el siguiente:

“Artículo 38 bis.- Infracciones leves. Se consideran infracciones leves las siguientes:

a) El incumplimiento total o parcial del deber de información y transparencia.

b) No disponer de un domicilio o de una dirección de correo electrónico o de un medio electrónico equivalente, actualizado y operativo, a través del cual los titulares de datos puedan dirigir sus comunicaciones o ejercer sus derechos.

c) No responder, responder en forma incompleta o responder fuera de plazo, las solicitudes formuladas por el titular de datos en conformidad a esta ley.

d) No informar o no remitir a la Agencia de Protección de Datos Personales las comunicaciones previstas en esta ley o en sus reglamentos.

e) No dar cumplimiento a las instrucciones generales impartidas por la Agencia de Protección de Datos Personales, que no estén sancionadas específicamente como infracción grave o gravísima.

f) Cometer cualquier otra infracción a los principios, derechos y obligaciones establecidas en esta ley, que no sea calificada como una infracción grave o gravísima.”.

Al iniciarse el estudio de este precepto, **el asesor del Honorable Senador señor Larraín, señor Olmedo,** consideró que el uso de la expresión negativa, al inicio de cada letra, no es adecuado.

El asesor del Comité Udi, señor Mery, criticó la amplitud de la letra f), al disponer: “Cometer cualquier otra infracción…”. Destacó que la conducta debe estar expresamente descrita en la ley.

El Presidente de la Comisión, Honorable Senador señor Harboe, coincidió en lo expresado por el señor Mery. Sin embargo, al utilizarse la expresión: “en esta ley”, se circunscribe a las infracciones a los principios, derechos y obligaciones consagrados en el cuerpo legal en estudio.

El asesor del Ministerio de Hacienda, señor Godoy, precisó que desde el punto de vista formal, y en base a lo observado por el asesor del Honorable Senador señor Larraín, se puede mejorar la redacción de este precepto.

En relación a la observación recaída en la letra f), precisó que en la presente iniciativa se ha dispuesto un conjunto de obligaciones a los responsables de datos, que no necesariamente están

recogidos en una infracción particular, porque de lo contrario tendría que elaborarse un catálogo más extenso.

El asesor del Comité Udi, señor Mery sugirió hacer una referencia a las normas, y no a los principios, ya que estos últimos pareciesen ser más imprecisos.

El Presidente de la Comisión, Honorable Senador señor Harboe manifestó que en la ley N° 20.900, para el fortalecimiento y transparencia de la democracia, se replica la norma contenida en la letra f), sin mencionar el término “principios”.

Asimismo, sugirió reemplazar el concepto “principios”, por “normas”.

En virtud de las observaciones precedentes, **el señor Presidente de la Comisión** sometió a votación la siguiente redacción:

Artículo 38 bis.- Infracciones leves. Se consideran infracciones leves las siguientes:

a) Incumplimiento total o parcial del deber de información y transparencia.

b) Carecer de un domicilio o de una dirección de correo electrónico o de un medio electrónico equivalente, actualizado y operativo, a través del cual los titulares de datos puedan dirigir sus comunicaciones o ejercer sus derechos.

c) Omitir la respuesta, responder en forma incompleta o fuera de plazo, las solicitudes formuladas por el titular de datos en conformidad a esta ley.

d) Omitir el envío a la Agencia de Protección de Datos Personales las comunicaciones previstas obligatoriamente en esta ley o sus reglamentos.

e) Incumplimiento de las instrucciones generales impartidas por la Agencia de Protección de Datos Personales en los casos que no esté sancionado como infracción grave o gravísima.

f) Cometer cualquier otra infracción a los derechos y obligaciones establecidas en esta ley, que no sea calificada como una infracción grave o gravísima.

La Comisión, por la unanimidad de sus miembros presentes, **Honorables Senadores señores Araya, Harboe y Larraín, aprobó esta redacción.**

Artículo 38 ter

En seguida, la Comisión analizó la propuesta del Ejecutivo de agregar un artículo 38 ter a la ley N° 19.628, referido a las infracciones graves. Su texto es el siguiente:

"Artículo 38.- ter.- Infracciones graves. Se consideran infracciones graves las siguientes:

a) Tratar los datos personales sin contar con el consentimiento del titular de datos o sin una base que otorgue licitud al tratamiento, o tratarlos con una finalidad distinta de aquella para la cual fueron recolectados.

b) Comunicar o ceder datos personales del titular sin su consentimiento, siendo necesario contar con aquel o cederlos para un fin distinto del autorizado.

c) Vulnerar los principios de proporcionalidad, calidad, seguridad o responsabilidad.

d) Impedir u obstaculizar el ejercicio legítimo de los derechos de acceso, rectificación, cancelación, oposición o portabilidad del titular.

e) No dar respuesta oportuna a una solicitud fundada de bloqueo temporal de los datos personales de un titular o denegar la solicitud sin causa justificada.

f) Realizar tratamiento de datos personales de niños, niñas y adolescentes con infracción a las normas previstas en esta ley.

g) Realizar tratamiento de datos personales sin cumplir los requisitos establecidos para las personas jurídicas de derecho privado sin fines de lucro y cuya finalidad sea política, filosófica, religiosa, cultural, sindical o gremial, respecto de los datos de sus asociados.

h) Vulnerar el deber de secreto o confidencialidad establecido en el artículo 14 bis.

i) No adoptar las medidas de seguridad que resulten adecuadas, necesarias y oportunas para el tratamiento de datos y que se encuentren previstas en esta ley o en el reglamento respectivo.

j) No efectuar las comunicaciones o no realizar los registros correspondientes en los casos de vulneración de las medidas de seguridad, según lo establecido en el artículo 14 quinquies.

k) Adoptar medidas de calidad y seguridad insuficientes o no idóneas para el tratamiento de datos personales con fines históricos, estadísticos o científicos y para estudios o investigaciones que atiendan fines de interés público.

l) Realizar operaciones de transferencia internacional de datos en contravención a las normas previstas en esta ley.

m) No dar cumplimiento a una resolución o un requerimiento específico y directo que le haya impartido la Agencia de Protección de Datos Personales.

n) La reiteración de infracciones leves.”.

Al iniciarse el estudio de esta disposición, **el asesor del Honorable Senador Larraín, señor Olmedo,** sugirió que la reiteración de infracciones leves se limite a un período de tiempo determinado.

El asesor del Ministerio de Hacienda, señor Godoy, hizo presente que en el inciso penúltimo del artículo 40 de la presente iniciativa, se define la reiteración. Esta norma dispone:

“Se entenderá que hay reiteración o reincidencia, cuando existan dos o más sanciones ejecutoriadas impuestas en virtud de la presente ley, en un período de 24 meses.”.

El asesor del Comité PPD, señor Abarca consideró que debido a la duración de los procedimientos, es bastante improbable que las sanciones se encuentren ejecutoriadas en un plazo de dos años.

El asesor del Ministerio de Hacienda, señor Godoy, precisó que dependiendo del procedimiento, se puede encontrar ejecutoriada en sede administrativa o judicial.

El Presidente de la Comisión, Honorable Senador señor Harboe, propuso eliminar el término “ejecutoriadas” y sugirió que la reiteración diga relación con la sanción impuesta por la Agencia.

El Honorable Senador señor Araya consignó que al no estar ejecutoriada la sanción, puede ocurrir que la resolución judicial revoque la decisión de la Agencia.

El Honorable Senador señor Larraín manifestó que la expresión “ejecutoriada” se refiere a un tema judicial. En todo caso, indicó que es efectivo que las sanciones emanan de la Agencia y de los tribunales.

El asesor del Ministerio de Hacienda, señor Godoy, expresó que se está pensando en cualquier sanción que se encuentre ejecutoriada. Es decir, una sanción aplicada por la Agencia y no reclamada por el infractor, o una sanción reclamada judicialmente, que ha quedado firme.

El Presidente de la Comisión, Honorable Senador señor Harboe insistió que es muy poco probable que en dos años las sanciones se encuentren ejecutoriadas.

El asesor del Ministerio de Hacienda, señor Godoy connotó que se podría extender el período de 24 meses.

Seguidamente, **el Presidente de la Comisión, Honorable Senador señor Harboe,** observó que la vulneración del deber de secreto o confidencialidad, consagrado en la letra h), puede provocar una afectación grave de la honra y dignidad de las personas. Constató que el daño puede ser extremadamente alto.

Agregó que la ley le ha dado el carácter de secreto a determinado tipo de datos y actuaciones. Lo anterior con la finalidad de resguardar la honra y la dignidad de los individuos.

Expresó que cuando los funcionarios o un tercero, están conminados a mantener un secreto, y lo vulneran, dicha infracción debiese estar en el catálogo de infracciones gravísimas.

El asesor del Ministerio de Hacienda, señor Godoy destacó que la letra d), del artículo 38 quater dispone lo siguiente:

“d) Vulnerar, a sabiendas, el deber de secreto o confidencialidad sobre los datos personales sensibles y datos personales relativos a la comisión y sanción de infracciones penales, civiles, administrativas y disciplinarias.”.

El Presidente de la Comisión, Honorable Senador señor Harboe apuntó que es partidario de eliminar, en el artículo

siguiente, las expresiones “maliciosamente” y “a sabiendas”. Hizo presente que probar el dolo en sede jurisdiccional será muy complejo, y el daño ya se habrá provocado. Estuvo de acuerdo en que se configure una responsabilidad objetiva. Es decir, se produce la conducta, se aplica la sanción.

El asesor del Ministerio de Hacienda, señor Godoy, reconoció que la vulneración de secreto es una conducta grave. Admitió que la sanción será la misma si se vulnera el deber de secreto por culpa o dolo.

El Presidente de la Comisión, Honorable Senador señor Harboe preguntó si se aplicará la misma sanción para el que vulnere el deber de secreto y para el que no adopte medidas de calidad y seguridad insuficientes o no idóneas para el tratamiento de datos personales con fines históricos, estadísticos o científicos y para estudios o investigaciones que atiendan fines de interés público.

Reiteró que se debe ser más riguroso cuando se infrinja el deber de secreto. Consultó cómo se crea un incentivo positivo para que las empresas tengan la obligación de cumplir con la protección del secreto. Estimó que la información que se revele se circunscribirá a datos sensibles.

El asesor del Comité Udi, señor Mery, manifestó que en la letra c), se habla de vulnerar los principios de proporcionalidad, calidad, seguridad o responsabilidad. Se mostró partidario de reemplazar la expresión “principios”, por “normas”.

Agregó que en relación a la letra n), que se refiere a la reiteración de infracciones leves, sostuvo que una misma conducta constituirá infracción y a la vez, reiteración.

En esta etapa del debate se sugirió sustituir la letra c) por las siguientes letras c) y d), nuevas:

“c) Efectuar tratamiento de datos personales innecesarios en relación con los fines del tratamiento.

d) Tratar datos personales inexactos, incompletos o desactualizados en relación con los fines del tratamiento.”

Puestas en votación las letras a), b), c) d), e), f), g), i), j), k), l) y m), del artículo 38 ter, fueron aprobadas por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Araya, Harboe y Larraín.

Respecto a la letra h) que pasa a ser letra i), **el asesor del Ministerio de Hacienda, señor Godoy** coincidió en que la vulneración del deber de secreto o confidencialidad puede llegar a ser significativa, al igual que la sanción.

Advirtió que en este caso no se debe configurar una sanción eventualmente desproporcionada por la cantidad de situaciones que pueden producirse de vulneración del deber de secreto o confidencialidad. Estas obligaciones no solo recaen sobre la persona que administra la Agencia, sino sobre todos los dependientes de dicho órgano.

Puesta en votación la letra h) –que pasa a ser i)-, fue aprobada por el voto favorable de los Honorables Senadores, señores Araya y Larraín. Se abstuvo el Honorable Senador, señor Harboe.

En relación a la letra n), que considera infracción grave la reiteración de infracciones leves, **el asesor del Ministerio de Hacienda, señor Godoy**, destacó que en el catálogo original de infracciones presentado por el Ejecutivo, no se consideraba como infracción grave la reiteración de infracciones leves. Ella fue incorporada fruto del trabajo técnico realizado con los asesores. Se mostró partidario de considerarla como agravante.

El asesor del Honorable Senador Larraín, señor Olmedo, hizo presente que cuando se transita a las infracciones gravísimas, todas ellas requieren dolo. Por lo tanto, el nivel de prueba es significativo.

Añadió que si no se genera un régimen sancionatorio eficiente y que permita un carácter preventivo, se debilita lo construido.

Concluido el debate de esta letra, el señor Presidente la Puso en votación.

La Comisión, por mayoría votos rechazó la letra n). Se pronunciaron en contra los Honorables Senadores señores Araya y Harboe. A favor lo hizo el Honorable Senador señor Larraín.

El texto acordado precedentemente fue ratificado mediante una indicación que presentó el Ejecutivo, la que se dio por aprobada con las votaciones señaladas precedentemente.

Artículo 38 quater

Seguidamente, la Comisión se abocó al análisis de la proposición del Gobierno de incorporar a la ley N° 19.628, un artículo 38 quater que estatuye las conductas que serán consideradas infracciones gravísimas. Su texto es el siguiente:

“Artículo 38 quater- Infracciones gravísimas. Se consideran infracciones gravísimas las siguientes:

a) Efectuar tratamiento de datos personales en forma fraudulenta.

b) Destinar maliciosamente los datos personales a una finalidad distinta de la consentida por el titular o prevista en la ley que autoriza su tratamiento.

c) Comunicar, transmitir o ceder, a sabiendas, información no veraz, incompleta, inexacta o desactualizada sobre el titular de datos.

d) Vulnerar, a sabiendas, el deber de secreto o confidencialidad sobre los datos personales sensibles y datos personales relativos a la comisión y sanción de infracciones penales, civiles, administrativas y disciplinarias.

e) Tratar, comunicar o ceder, a sabiendas, datos personales sensibles o datos personales de niños, niñas y adolescentes, en contravención a las normas de esta ley.

f) Recolectar maliciosamente a través de niños, niñas o adolescentes, datos personales de los integrantes de su grupo familiar.

g) No comunicar oportunamente, habiendo estado en conocimiento de ello y disponiendo de los medios para hacerlo, la vulneración de las medidas de seguridad que puedan afectar la confidencialidad, disponibilidad o integridad de los datos personales.

h) Efectuar tratamiento masivo de datos personales contenidos en registros electrónicos de infracciones penales, civiles, administrativas y disciplinarias, que llevan los organismos públicos, sin contar con autorización legal para ello.

i) Realizar maliciosa o negligentemente operaciones de transferencia internacional de datos en contravención a las normas previstas en esta ley.

j) No dar cumplimiento a una resolución de la Agencia de Protección de Datos Personales que resuelve la reclamación de un titular sobre el ejercicio de sus derechos de acceso, rectificación, cancelación, oposición, portabilidad o bloqueo temporal.

k) Entregar información falsa, incompleta o manifiestamente errónea en el proceso de registro o certificación del modelo de prevención de infracciones.

l) La reiteración de infracciones graves.”

Al comenzar el debate de esta disposición, **el asesor del Ministerio de Hacienda, señor Godoy,** manifestó, en relación a la letra d), que estamos ante un tipo particular de datos personales sensibles y de datos personales relativos a la comisión y sanción de infracciones penales, civiles, administrativas y disciplinarias. Agregó que estos antecedentes requieren un mayor nivel de protección jurídica, una vulneración de esa información, sin importar que pueda existir un elemento intencional debería ser calificada como infracción gravísima. Debido a lo anterior, sugirió eliminar la expresión: “a sabiendas”.

El Presidente de la Comisión, Honorable Senador señor Harboe, hizo presente que la letra f), sanciona a quien recolecte maliciosamente a través de niños, niñas o adolescentes, datos personales de los integrantes de su grupo familiar. Recalcó que quien busca obtener el consentimiento de un menor de edad para proveerse de información respecto a la familia del niño, niña o adolescente, sabe que está en presencia de un consentimiento que carece de valor. Sugirió eliminar la expresión “maliciosamente”.

El Honorable Senador señor Larraín propuso que, atendida la complejidad de las normas en revisión, un profesor de derecho penal revise el conjunto de sanciones consagradas.

El asesor del Ministerio de Hacienda, señor Godoy sostuvo que se puede eliminar la letra f), ya que ésta quedaría comprendida en las hipótesis configuradas en las letras a) y b).

Hizo presente que no resulta conveniente suprimir la expresión “maliciosamente”. Puso el ejemplo de un menor que se encuentre extraviado, y un adulto le solicita el número de teléfono de su padre para comunicarse con este último. Subrayó que en ciertas situaciones de emergencia es imprescindible requerir información de parte del niño, niña o adolescente.

En esta parte del debate, el Ejecutivo retiró la letra f), del artículo 38 quáter.

En cuanto a la letra i), **el asesor del Comité Udi, señor Mery**, demostró su disconformidad en que se incorpore la expresión “negligentemente”. Precisó que dicho término no está presente en las otras categorías de infracciones gravísimas.

El asesor del Ministerio de Hacienda, señor Godoy reconoció que es la única letra de las infracciones gravísimas en que se incorpora el actuar negligente. Explicó que ello es así, porque cuando se produce el efecto de transferencia internacional se pierde todo tipo de control respecto de los datos.

El Presidente de la Comisión, Honorable Senador señor Harboe, consignó que estamos en el ámbito del derecho sancionatorio administrativo.

El Honorable Senador señor Larraín constató que la negligencia constituye un elemento que debe ser considerado dentro de las sanciones graves. Agregó que la malicia y el dolo, deben circunscribirse a las sanciones gravísimas.

El Presidente de la Comisión, Honorable Senador señor Harboe, connotó que estamos en presencia de protección de datos personales y no de actos administrativos físicos. Añadió que puede ocurrir que la transferencia internacional de datos se realice digitalmente. Preguntó cómo se entera el titular de dicha transferencia. Asimismo, inquirió cómo se puede probar que quien transfirió los datos lo hizo actuando maliciosa o negligentemente.

Sugirió mantenerla como infracción gravísima, o eliminar los términos “maliciosa o negligentemente” y configurar la responsabilidad objetiva.

El Honorable Senador señor Larraín enfatizó que no se puede sancionar de la misma manera la malicia de la negligencia.

Concluido el estudio de esta materia, el señor Presidente de la Comisión la sometió a votación.

Puestas en votación las letras a, b, c, d, e, g, h, j, k, del artículo 38 quater, fueron aprobadas por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Araya, Harboe y Larraín.

A continuación, se analizó la propuesta del Honorable Senador, señor Larraín de reemplazar en la letra i), las expresiones: “maliciosa o negligentemente”, por: “a sabiendas”.

Puesta en votación le letra i), que pasa a ser letra h) como consecuencia del retiro de la letra f), con la enmienda señalada, fue aprobada por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Araya, Harboe y Larraín.

Puesta en votación la letra l), fue rechazada con el voto unánime de los Honorables Senadores señores Araya, Harboe y Larraín.

El texto acordado precedentemente fue ratificado mediante una indicación que presentó el Ejecutivo, la que se dio por aprobada con las votaciones señaladas precedentemente.

Artículo 39

Seguidamente, la Comisión consideró el artículo 39 del proyecto de ley del Ejecutivo, que establece el régimen de sanciones que se puede imponer a quienes cometan los distintos tipos de infracciones ya descritas. El texto de esta disposición es el siguiente:

“Artículo 39.- Sanciones. Las sanciones a las infracciones en que incurran los responsables de datos serán las siguientes:

a) Las infracciones leves serán sancionadas con amonestación escrita o multa de 1 a 50 unidades tributarias mensuales.

b) Las infracciones graves serán sancionadas con multa de 51 a 500 unidades tributarias mensuales.

c) Las infracciones gravísimas serán sancionadas con multa de 501 a 5.000 unidades tributarias mensuales.”.

En relación a esta materia se tuvo presente que la moción parlamentaria que se refunde en este informe, establece el siguiente régimen de sanciones:

“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.”.

El Presidente de la Comisión, Honorable Senador señor Harboe, sugirió eliminar el monto mínimo de la multa en caso de infracciones graves y gravísimas. Ejemplificó con el caso de una pequeña empresa a la que se le impone una multa de 51 UTM por haber cometido una infracción grave, lo que podrá significar una afectación grave a su fuente laboral.

Añadió que sugería eliminar el piso de la multa porque la ponderación de ella la realizaría la Agencia o el juez, según corresponda, tomando en consideración el tipo de infractor.

Los representantes del Ejecutivo hicieron presente que no compartía ese criterio. Insistieron en aprobar la formula contenida en el proyecto de ley del Ejecutivo.

El asesor del Ministerio de Hacienda, señor Godoy destacó que existe un conjunto de elementos a considerar al momento de determinar la multa. Añadió que el principio de proporcionalidad constituye la inspiración para mantener los pisos de las multas. Ejemplificó con el caso en que una infracción grave puede ser sancionada con una multa similar al que cometa una infracción leve si se eliminan los pisos de cada tramo de multa.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, De Urresti y Harboe, aprobó el artículo 39 propuesto por el Ejecutivo.

Artículos 40 y 41

A continuación, la Comisión trató conjuntamente los artículos 40 y 41 del proyecto de ley del Ejecutivo, preceptos que establecen las reglas para determinar el monto de las multas y las circunstancias atenuantes de responsabilidad. El texto de ambas disposiciones es el siguiente:

“Artículo 40.- Determinación del monto de las multas. La cuantía de la multa, dentro del rango asignado para cada tipo de

infracción, será determinada por la Agencia de Protección de Datos Personales teniendo en cuenta los siguientes criterios:

a) La conducta realizada por el responsable y la naturaleza de la infracción.

b) Si la conducta fue realizada por el responsable de datos con falta de diligencia o cuidado, a sabiendas o maliciosamente.

c) Si el infractor es una persona natural o jurídica.

d) Si se trata de una fundación, asociación o cualquier otra entidad que no persiga fines de lucro y cuya finalidad sea política, filosófica, religiosa, sindical o gremial.

e) En el caso de las empresas se debe tener en cuenta el monto de las ventas de la empresa infractora conforme a lo dispuesto en el artículo 16 de la ley Nº 20.416.

f) El perjuicio producido con motivo de la infracción, especialmente el número de titulares de datos que se vieron afectados.

g) Los beneficios obtenidos por el responsable a consecuencia de la infracción.

h) La conducta anterior del responsable, la reiteración de los hechos y el carácter continuado de la infracción.

i) La existencia de circunstancias atenuantes de responsabilidad o de atenuantes calificadas.

Cuando concurran circunstancias atenuantes, la Agencia de Protección de Datos Personales estará autorizada para rebajar la sanción que corresponda a la infracción cometida dentro del rango respectivo o aplicar la sanción prevista para una infracción de menor gravedad. Cuando concurran atenuantes calificadas de responsabilidad, la Agencia de Protección de Datos Personales podrá, además, exonerar la conducta del infractor.

En caso que exista reiteración o reincidencia, la Agencia de Protección de Datos Personales puede aplicar una multa de hasta tres veces el monto señalado en el artículo anterior, según corresponda al tipo de infracción cometida.

Se entenderá que hay reiteración o reincidencia, cuando existan dos o más sanciones ejecutoriadas impuestas en virtud de la presente ley, en un período de 24 meses.

En caso que se verifique la concurrencia de dos o más infracciones de la misma naturaleza, se aplicará la sanción correspondiente a la infracción más grave, estimándose los hechos constitutivos de una sola infracción. Si atendida la naturaleza y gravedad de las infracciones, éstas no pueden estimarse como una sola, se acumularán las sanciones correspondientes a cada una de las infracciones concurrentes.”.

Artículo 41.- Atenuantes de responsabilidad. Se consideran circunstancias atenuantes de responsabilidad las acciones unilaterales de reparación que realice el responsable de datos y los acuerdos reparatorios convenidos con los titulares de datos afectados.

Constituyen también atenuantes de responsabilidad la conducta anterior del responsable de datos y la colaboración que preste en la investigación administrativa que practique la Agencia de Protección de Datos Personales.

Si el infractor detecta que ha cometido o está cometiendo una infracción a los principios y obligaciones que establece esta ley, podrá autodenunciarse ante la Agencia de Protección de Datos Personales. En esa misma oportunidad, el infractor deberá comunicar las medidas adoptadas para el cese de los hechos que originaron la infracción o las medidas de mitigación adoptadas, según corresponda. La autodenuncia será considerada como una atenuante calificada de responsabilidad.

También constituye una atenuante calificada de responsabilidad que el responsable acredite haber cumplido diligentemente sus deberes de dirección y supervisión para la protección de los datos personales sujetos a tratamiento, lo que se verificará con el certificado expedido de acuerdo a lo dispuesto en el artículo 53 de esta ley.

Al iniciarse el estudio de esta materia, se tuvo presente que la moción parlamentaria que se refunde en este informe también establece un conjunto reglas para la determinación de las sanciones. Su texto es el siguiente:

“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.”.

Al examinarse estas disposiciones, **el asesor del Comité Udi, señor Mery,** manifestó que en el inciso 1º del artículo 40 se hace referencia a la Agencia de Protección de Datos Personales, como aquella que puede determinar la cuantía de la multa. Precisó que si hay revisión judicial, será la Corte de Apelaciones respectiva la que establezca la multa. De este modo la referencia expresa a la Agencia, circunscribe la posibilidad de que solo ella determine el monto de la multa.

Sugirió eliminar la mención a la Agencia de Protección de Datos Personales al momento de determinar la multa.

El asesor del Ministerio de Hacienda, señor Godoy hizo presente que en la letra h), del artículo 47 del proyecto de ley del Ejecutivo se señala: “h) Tratándose de reclamaciones en contra de una resolución que resuelve un procedimiento sancionatorio, la Corte podrá confirmar o revocar la resolución impugnada, establecer o desechar la

comisión de la infracción, según corresponda y, mantener, dejar sin efecto o modificar la sanción impuesta al responsable.

En seguida, la Comisión examinó el artículo 41 del proyecto de ley del Ejecutivo.

El asesor del Ministerio de Hacienda, señor Godoy, manifestó que en el artículo 41 se consignan condiciones que atenúan las obligaciones del responsable de datos frente a una infracción. Precisó que éstas facultan a la Agencia a rebajar la sanción.

Subrayó que la regla de aplicación de las sanciones se consagra en el artículo 40. El inciso segundo señala: “Cuando concurran circunstancias atenuantes, la Agencia de Protección de Datos Personales estará autorizada para rebajar la sanción que corresponda a la infracción cometida dentro del rango respectivo o aplicar la sanción prevista para una infracción de menor gravedad. Cuando concurran atenuantes calificadas de responsabilidad, la Agencia de Protección de Datos Personales podrá, además, exonerar la conducta del infractor.”.

Estimó que hay elementos que deben ser ponderados al momento de aplicar la sanción. Asimismo, afirmó que habrá ocasiones en que existiendo una atenuante calificada, la infracción podrá ser reducida y puede llegar a la sanción más baja, constituida por la amonestación.

El Presidente de la Comisión, Honorable Senador señor Harboe se mostró partidario que sea facultativo para la Agencia rebajar la sanción. Consideró que sería un exceso establecer la obligación de rebajarla.

La asesora del Honorable Senador señor De Urresti, señora Melissa Mallega, manifestó que se debiera modificar el texto del Mensaje, ya que en él se contempla la posibilidad que si concurren atenuantes calificadas de responsabilidad, la Agencia de Protección de Datos Personales podía exonerar la conducta del infractor.

El asesor del Honorable Senador Larraín, señor Olmedo consultó de qué manera podría estar consagrándose en este artículo la autodenuncia dolosa, para efectos de evitar otro tipo de investigaciones.

El asesor del Ministerio de Hacienda, señor Godoy, recordó lo establecido en el artículo 38, inciso segundo que inaugura el párrafo sobre responsabilidad. Este precepto prescribe: “Las responsabilidades en que incurra una persona natural o jurídica por las

infracciones establecidas en esta ley, se entienden sin perjuicio de las demás responsabilidades legales, civiles o penales, que pudieran corresponderle.”

Agregó que la responsabilidad infraccional no obsta a que, por ejemplo, exista alguna conducta constitutiva de delito, que deba perseguirse en sede penal.

Destacó que el único efecto que produce la autodenuncia es que permite aminorar la pena. Aseveró que con ello se busca incentivar el cumplimiento de parte de los responsables de datos. Consignó que para que la autodenuncia no se transforme en una figura abusiva, se le impone una restricción, que consiste en que respecto de las infracciones gravísimas esta atenuante calificada solo puede utilizarse en una sola oportunidad.

El Presidente de la Comisión, Honorable Senador señor Harboe, constató que cuando se habla de autodenuncia, también se debe pensar en una figura similar a la delación compensada, que permite que no solo se denuncie respecto de un hecho propio. Esto último puede significar un mecanismo de información para la Agencia, que permita detectar infracciones. Recalcó que una figura como la descrita, podría ayudar a la institucionalidad pública a tomar conocimiento de ciertas infracciones y a investigarlas como corresponde.

Remarcó que en Chile, la mayoría de los casos en que se ha detectado casos de colusión ha sido gracias a la delación compensada. Añadió que el sistema de inteligencia financiero es muy precario.

En una sesión posterior, **los representantes del Ejecutivo** propusieron a la Comisión cambiar el orden de estas normas, con el fin de regular en el artículo 40 las circunstancias atenuantes y agravantes de responsabilidad y en el artículo 41 las reglas para la determinación del monto de las multas. El texto de estas disposiciones es el siguiente:

“Artículo 40.- Circunstancias atenuantes y agravantes de responsabilidad**.** Se considerarán circunstancias atenuantes:

a) Las acciones unilaterales de reparación que realice el responsable y los acuerdos reparatorios convenidos con los titulares de datos que fueron afectados

b) La colaboración que el infractor preste en la investigación administrativa practicada por la Agencia de Protección de Datos Personales.

c) La ausencia de sanciones previas del responsable de datos.

d) La autodenuncia ante la Agencia de Protección de Datos Personales. Junto con la autodenuncia el infractor deberá comunicar las medidas adoptadas para el cese de los hechos que originaron la infracción o las medidas de mitigación implementadas, según corresponda.

e) El haber cumplido diligentemente sus deberes de dirección y supervisión para la protección de los datos personales sujetos a tratamiento, lo que se verificará con el certificado expedido de acuerdo a lo dispuesto en el artículo 53 de esta ley.

Se considerarán circunstancias agravantes:

a) La reincidencia. Existe reincidencia, cuando el responsable ha sido sancionado en dos o más ocasiones, en los últimos 30 meses, por infracción a esta ley. Las resoluciones que aplican las sanciones respectivas deberán encontrarse firme o ejecutoriadas.

b) El carácter continuado de la infracción.

c) El haber puesto en riesgo la seguridad de los titulares de los datos personales.

Artículo 41.- Determinación del monto de las multas**.** Para la determinación del monto de las multas señaladas en esta ley, la Agencia de Protección de Datos Personales deberá aplicar las reglas señaladas en los incisos siguientes.

La Agencia de Protección de Datos Personales deberá ponderar racionalmente cada una de las atenuantes y agravantes a fin de que se aplique al caso concreto una multa proporcional a la intensidad de la afectación.

Cuando solo concurran circunstancias atenuantes de responsabilidad, la Agencia de Protección de Datos Personales estará autorizada para aplicar al responsable, aquella sanción prevista para una infracción de menor gravedad. En los casos de las circunstancias atenuantes establecidas en las letras d) y e) del artículo anterior, la Agencia de Protección de Datos Personales podrá rebajar la sanción hasta amonestación, salvo cuando se trate de la autodenuncia de infracciones gravísimas, en cuyo caso esta rebaja sólo tendrá efecto para la primera ocasión.

En caso de que exista reincidencia, la Agencia de Protección de Datos Personales podrá aplicar una multa de hasta tres veces el monto asignado a la infracción cometida.

Efectuada la ponderación señalada en los incisos anteriores, y para establecer el monto específico de la multa, se considerarán prudencialmente los siguientes criterios:

a) Si la conducta fue realizada por el responsable con falta de diligencia o cuidado, a sabiendas o maliciosamente, en aquellos casos que no se consideran estos elementos en la configuración de la infracción;

b) Si se trata de una persona jurídica de derecho privado que no persiga fines de lucro, se deberá tener en cuenta su capacidad económica;

c) Si se trata de una empresa, se deberá considerar el monto de sus ventas conforme a lo dispuesto en el artículo 16 de la ley Nº 20.416;

d) El perjuicio producido con motivo de la infracción, especialmente el número de titulares de datos que se vieron afectados;

e) Los beneficios obtenidos por el responsable a consecuencia de la infracción, y

f) Si el tratamiento realizado incluye datos personales sensibles o datos personales de niños, niñas y adolescentes.

En caso de que se verifique la concurrencia de dos o más infracciones de la misma naturaleza, se aplicará la sanción correspondiente a la infracción más grave, estimándose los hechos constitutivos de una sola infracción. Si atendida la naturaleza y gravedad de las infracciones, éstas no pueden estimarse como una sola, se acumularán las sanciones correspondientes a cada una de las infracciones concurrentes.”.

Al explicar estas normas, **el asesor del Ministerio de Hacienda, señor Godoy,** hizo presente que tanto las atenuantes como las agravantes que están expresadas en la presente disposición, son las contenidas en el artículo 40, que ya conoció la Comisión.

Remarcó que en esta nueva propuesta, en un mismo artículo, se separan las atenuantes de las agravantes. Agregó que en un artículo distinto se consagran los elementos para determinar las multas.

El Presidente de la Comisión, Honorable Senador señor Harboe recordó que se había planteado como atenuante el adoptar medidas internas para resguardar los datos.

El asesor del Ministerio de Hacienda, señor Godoy remarcó que ello se consagra en la letra e) del nuevo artículo 40.

El Presidente de la Comisión, Honorable Senador señor Harboe preguntó si se eliminó a la autodenuncia como atenuante calificada.

El asesor del Ministerio de Hacienda, señor Godoy precisó que las reglas de aplicación de la multa se encuentran en el artículo siguiente.

En relación a las agravantes, **el Honorable Senador, señor Araya** estimó que la agravante consagrada en la letra b), a saber, el carácter continuado de la infracción, debiera ser una regla de determinación del monto de la multa, más que una agravante.

El asesor del Comité Udi, señor Mery, sostuvo que la continuidad de la infracción está ligada al comportamiento básico.

El asesor del Ministerio de Hacienda, señor Godoy, respecto al carácter continuado de la infracción, manifestó que la continuidad no constituye una base para el tratamiento de datos.

Añadió que ella, a diferencia de la reincidencia, si se realiza durante un largo periodo de tiempo causa un mayor perjuicio y agravio al afectado. Añadió que estamos en presencia de titulares que estuvieron expuestos al daño por un período largo de tiempo.

El Honorable Senador, señor Araya constató que al concurrir las atenuantes de las letras d) y e) del artículo anterior, se rebaja la sanción hasta la amonestación, salvo que se trate de infracciones gravísimas. Propuso que solo se aplique el mencionado beneficio respecto a las infracciones leves, a menos que se exija que concurran copulativamente ambas atenuantes.

El asesor del Ministerio de Hacienda, señor Godoy, respondió que es central el modelo de cumplimiento en la presente iniciativa. Expresó que existirán instituciones que carecen del nivel de complejidad para efectos de desarrollar dichos modelos.

Agregó que para ese tipo de instituciones, el modelo de autodenuncia es muy relevante. Para que ocurra lo anterior, debe haber un incentivo importante. Recalcó que si éste se rebaja, se debilitan las posibilidades efectivas de cumplimiento de la ley.

El Honorable Senador señor Araya advirtió que puede ocurrir el absurdo que una empresa se autodenuncia, luego hace uso del beneficio y trata datos personales sin el consentimiento del titular, lo que le significará solo una sanción de amonestación.

Sugirió que se aplique el piso de la multa de acuerdo a la infracción. Reiteró que en el caso de las infracciones graves, la empresa, con la finalidad de rebajar la sanción, seguirá el camino de la autodenuncia.

El asesor del Ministerio de Hacienda, señor Godoy sostuvo que en la letra d) del artículo 40, lugar donde se regula la autodenuncia como atenuante, establece exigencias. Ellas consisten en que junto con la autodenuncia, el infractor deberá comunicar las medidas adoptadas para el cese de los hechos que originaron la infracción o las medidas de mitigación implementadas, según corresponda.

Atendido lo anterior, consignó que no basta con autodenunciarse. Recalcó que debe ir acompañada de acciones correctivas o de reparación, según corresponda. Agregó que respecto a las infracciones gravísimas, la autodenuncia solo la primera vez producirá el efecto de rebajar la sanción al límite inferior.

El Honorable Senador señor Araya hizo presente que la empresa, en el caso de infracciones graves y gravísimas, obtendrá un beneficio económico producto del tratamiento de esos datos.

Subrayó que en esos casos, la amonestación termina siendo un premio para la empresa infractora.

El Presidente de la Comisión, Honorable Senador señor Harboe, acotó que dentro de las circunstancias que se consideran necesarias para que la autodenuncia sea aceptada como una atenuante se deben comunicar las medidas para el cese de la infracción o haber mitigado los impactos. Constató que si esa es una circunstancia que está implícita en la letra d), podrá entenderse que dicha mitigación haga concurrir además, la atenuante de la letra a).

El asesor del Ministerio de Hacienda, señor Godoy concordó con lo señalado por el Presidente de la Comisión.

Para resolver lo planteado, propuso incorporar un límite a las infracciones graves y gravísimas.

El Presidente de la Comisión, Honorable Senador señor Harboe observó que debe establecerse que la concurrencia de la causal de mitigación de la letra d), no dice relación con la consagrada en la letra a).

Por otra parte, agregó que en la letra c) del artículo 41 se hace referencia, para fijar la multa, al monto de las ventas. Se

mostró contrario a implementar dicho criterio, porque el mencionado volumen puede no revelar la capacidad económica de una empresa.

Sugirió hablar de capacidad económica.

El asesor del Honorable Senador Larraín, señor Olmedo propuso a la Comisión eliminar la letra c), y suprimir en la letra b) del artículo 41, la expresión: “que no persiga fines de lucro”.

Concluido el estudio de ambas disposiciones, fueron sometidas a votación por el señor Presidente de la Comisión.

La Comisión, por la unanimidad de sus miembros presentes, los Honorables Senadores señores Araya, De Urresti y Harboe, aprobó los nuevos artículos 40 y 41 propuestos por el Ejecutivo, con las siguientes enmiendas:

1. Eliminar en la letra b) del artículo 41 la frase “que no persiga fines de lucro”, y

2. Suprimir la letra c) del artículo 41.

Artículo 42

Seguidamente, la Comisión consideró el artículo 42 contenido en el proyecto de ley del Ejecutivo, que regula el tema de las sanciones accesorias que se pueden imponer a los infractores. Su texto es el siguiente:

“Artículo 42.- Sanciones accesorias. En caso que se impongan multas por infracciones graves o gravísimas reiteradas y existan circunstancias debidamente justificadas, la Agencia de Protección de Datos Personales podrá disponer la suspensión de las operaciones de tratamiento de datos por parte del responsable de datos hasta por un término de 30 días.

Durante el período de suspensión, el responsable de datos deberá adoptar las medidas necesarias a objeto de adecuar sus operaciones de tratamiento a las exigencias establecidas en la presente ley, de acuerdo a lo dispuesto en la resolución de la Agencia de Protección de Datos Personales que ordenó la suspensión.

Si el responsable no da cumplimiento a lo dispuesto en la resolución de suspensión, esta medida se podrá prorrogar por otros 30 días, hasta completar un período máximo de 6 meses de

suspensión. De persistir el incumplimiento, el responsable no podrá volver a desarrollar actividades de tratamiento de datos personales.

Cuando la suspensión afecte a una entidad sujeta a supervisión por parte de un organismo público de carácter fiscalizador, la Agencia de Protección de Datos Personales deberá previamente poner los antecedentes en conocimiento de la autoridad regulatoria correspondiente y coordinar con ella la aplicación de la sanción con el objeto de no afectar a los usuarios del servicio que será suspendido.”.

Al iniciarse el estudio de esta disposición, **los representantes del Ejecutivo, señora Piedrabuena y señor Godoy**, sugirieron a la Comisión aprobar el texto del Ejecutivo, enmendado en los siguientes términos:

“Artículo 42.- Sanciones accesorias. En caso que se impongan multas por infracciones gravísimas reiteradas, en un período de 24 meses, la Agencia de Protección de Datos Personales podrá disponer la suspensión de las operaciones y actividades de tratamiento de datos que realiza el responsable de datos, hasta por un término de 30 días.

Durante este período, el responsable deberá adoptar las medidas necesarias a objeto de adecuar sus operaciones y actividades a las exigencias dispuestas en la resolución que ordenó la suspensión.

Si el responsable no da cumplimiento a lo dispuesto en la resolución de suspensión, esta medida se podrá prorrogar indefinidamente, por períodos sucesivos de 30 días, hasta que el responsable cumpla con lo ordenado.

Cuando la suspensión afecte a una entidad sujeta a supervisión por parte de un organismo público de carácter fiscalizador, la Agencia de Protección de Datos Personales deberá previamente poner los antecedentes en conocimiento de la autoridad regulatoria correspondiente y coordinar con ella la aplicación de la sanción con el objeto de no afectar a los usuarios del servicio que será suspendido.”.

El señor Presidente de la Comisión concedió, en primer lugar, el uso de la palabra al **asesor del Ministerio de Hacienda, señor Godoy,** quien expresó que la presente norma, desde el punto de vista de los incentivos, es una de las disposiciones más importantes que considera este proyecto de ley. Agregó que la multa es disuasiva de aquellas infracciones que pueda cometer el responsable.

Insistió que la sanción más importante que contempla el proyecto de ley está constituida por la suspensión de las actividades de tratamiento de datos, por parte de aquellos responsables que incurren reiteradamente en infracciones gravísimas.

Afirmó que la suspensión durará, en tanto el responsable no adopte las medidas necesarias para corregir aquellas conductas que fueron motivo de la infracción.

El asesor del Honorable Senador Larraín, señor Olmedo, señaló que la resolución de suspensión podrá ser objeto de un reclamo judicial y de una orden de no innovar, lo cual plantea una situación compleja de probable enfrentamiento entre la Agencia y el Poder Judicial.

En relación al inciso final, consignó que se debe revisar la facultad fiscalizadora conjunta de la Agencia con la autoridad regulatoria correspondiente.

El Presidente de la Comisión, Honorable Senador señor Harboe, preguntó si se suspende al responsable o a la base de datos. Remarcó que esa discusión se ha dado a nivel internacional.

Añadió que cuando uno suspende al responsable la sanción recae sobre la persona jurídica que está realizando acciones de tratamiento. Mostró su preocupación respecto a cómo evitar que la persona natural, que está detrás de la persona jurídica, pueda seguir llevando a cabo las acciones sancionadas bajo otra figura.

El asesor del Comité del PPD, señor Sebastián Abarca consultó si la resolución que dicta la Agencia no puede ser impugnada. Agregó que si así fuese, estaríamos ante la herramienta más poderosa de dicho órgano.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena precisó que la suspensión recae sobre la actividad de tratamiento de datos.

Acotó que, de acuerdo a lo señalado por el asesor, señor Olmedo, es fundamental la coordinación entre el órgano regulador y la Agencia, ya que las consecuencias pueden ser perjudiciales para los usuarios.

El Presidente de la Comisión, Honorable Senador señor Harboe estimó que es conveniente que se coordinen. Sin embargo, hizo presente que no es partidario que ambas entidades se conjuguen para la aplicación de la sanción. Eso implica otorgarle a la

Agencia un rango inferior, no solo respecto al Consejo para la Transparencia, sino que también respecto a los reguladores sectoriales.

Aseveró que la potestad sancionadora corresponde al Director de la Agencia y no puede quedar sometida a lo que diga el regulador.

El asesor del Ministerio de Hacienda, señor Godoy hizo presente que en cuanto a la suspensión judicial, el inciso primero del artículo 47, establece que: “Las personas naturales o jurídicas que se vean afectadas o agraviadas por una resolución final o de término de la Agencia de Protección de Datos Personales podrán deducir un reclamo de ilegalidad ante la Corte de Apelaciones de Santiago o la del lugar donde se encuentre domiciliado el reclamante, a elección de este último la reclamación judicial…”.

Connotó que la aplicación de la suspensión, será parte de la resolución de término. Indicó que en nada afecta la autonomía de la Agencia el que esté sometida al control jurisdiccional.

Reconoció que será difícil resolver con el marco legal actual, si la persona natural sigue realizando operaciones de tratamiento de datos bajo una figura distinta a la de la persona jurídica que se encuentra sancionada.

En cuanto a la coordinación regulatoria, estimó que no hay dificultad en afinar la redacción. Sin embargo, manifestó que no se deben coordinar para efectos de aplicar la sanción, sino respecto a los efectos que ésta produce frente a los usuarios.

El Presidente de la Comisión, Honorable Senador señor Harboe sugirió la siguiente redacción al inciso final: “Cuando la suspensión afecte a una entidad sujeta a supervisión por parte de un organismo público de carácter fiscalizador, la Agencia de Protección de Datos Personales deberá previamente poner los antecedentes en conocimiento de la autoridad regulatoria correspondiente, para los efectos de cautelar los derechos de los usuarios de dicha entidad.”.

Sometido a votación el artículo 42, fue aprobado con esta última enmienda, por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Araya, Harboe y Larraín.

El texto acordado precedentemente fue ratificado mediante una indicación que presentó el Ejecutivo, la que se dio por aprobada con la votación señalada precedentemente.

Artículo 43

A continuación, la Comisión trató el artículo 43 del proyecto de ley del Ejecutivo que incorpora a la ley N° 19.628 el Registro Nacional de Cumplimiento y Sanciones. Su texto es el siguiente:

"Artículo 43.- Registro Nacional de Cumplimiento y Sanciones. Créase el Registro Nacional de Cumplimiento y Sanciones administrado por la Agencia de Protección de Datos Personales. El registro será público y su acceso gratuito. Se consultará y llevará en forma electrónica.

En este registro se deberán consignar a los responsables de datos que hayan sido sancionados por infringir los principios y obligaciones establecidos de esta ley, señalar la conducta infraccionada, las circunstancias atenuantes y agravantes de responsabilidad y la sanción impuesta.

Las anotaciones en el registro serán de acceso público por el período de 5 años a contar de la fecha en que se practicó la anotación.".

Al iniciarse el estudio de esta disposición, **el asesor del Ministerio de Hacienda, señor Godoy,** explicó que esta disposición crea un Registro Nacional que actuará como un incentivo al cumplimiento. Agregó que contendrá información sobre aquellos responsables de datos que infringen la ley. Puntualizó que ello permite que los consumidores, los ciudadanos y los usuarios, conozcan a las instituciones infractoras.

El asesor del Honorable Senador Larraín, señor Olmedo, mostró su preocupación por la extensión del plazo para acceder al mencionado Registro. Preguntó cómo se vincula esta regla con el derecho al olvido.

El asesor del Ministerio de Hacienda, **señor Godoy,** detalló que en el artículo 25, que regula los datos relativos a infracciones penales, civiles, administrativas y disciplinarias, se introdujo una regla que señala que todos aquellos registros de información que no tengan un plazo especial establecido en la ley, pueda permanecer disponibles hasta por un período de 5 años.

Atendido lo anterior, se consagró el mencionado plazo en el inciso final del artículo en estudio.

El asesor del Comité Udi, señor Mery, constató que el uso de la denominación derecho al olvido, para hablar de la supresión de datos en un registro, es complejo, porque las anotaciones son consecuencia de la aplicación de resoluciones. Admitió que ellas no se refieren a la vida privada, ni actos entre particulares, sino que corresponden a resoluciones de carácter punitivo pronunciadas por la Agencia.

Consultó si transcurrido los 5 años se produce una eliminación automática de la anotación, o existirá un procedimiento para que el interesado pueda requerir la eliminación de los antecedentes.

Expresó que como son actos de la autoridad, rige el principio de publicidad. Por lo tanto, enfatizó que la Agencia no puede rehusarse a entregar, después de transcurrido los 5 años, las decisiones y fundamentos del acto que se eliminó. Es decir, regiría la regla general de la transparencia.

Finalmente, recalcó que el hecho de que se elimine del registro no priva a las personas de pedir copia de los antecedentes que significaron la aplicación de una sanción.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena aseveró que estamos en presencia de un registro público. Es decir, las personas que hayan cometido una infracción van a estar en él durante 5 años. Agregó que cumplido ese lapso, se borra automáticamente la anotación. Lo anterior no quiere decir que el fiscalizador pueda conservar la información allí registrada.

El Presidente de la Comisión, Honorable Senador señor Harboe, sostuvo que el registro de infractores cumple el objetivo de informarle a la comunidad que hay un conjunto de personas naturales o jurídicas, que han infringido reiteradamente la Ley de Protección de la Vida Privada. Preguntó cuál es la sanción efectiva que implica estar en el registro. Consultó si, aparte de incorporarlo en el mencionado padrón, se impondrán multas al infractor, o quedará inhabilitado para ejercer como responsable de datos.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena recordó que se han establecido diversas sanciones administrativas, y una de ellas es la anotación en el registro. Agregó que este registro es público, gratuito, se llevará en forma electrónica y estará disponible en la página web de la Agencia.

El Presidente de la Comisión, Honorable Senador señor Harboe sugirió que se incorpore en el artículo en estudio el requisito de publicidad del registro en la página web de dicho órgano.

Asimismo, propuso que se agregue como sanción la inhabilidad para contratar con el Estado en el ámbito de la protección de datos.

El asesor del Ministerio de Hacienda, señor Godoy recalcó que la sanción más importante que posee el proyecto de ley en estudio es la de la suspensión. Recordó que si un responsable de datos infringe de manera reiterada sus obligaciones en el tratamiento de datos, sus operaciones serán suspendidas, lo que produce un importante impacto disuasivo.

Asimismo, agregó que en esta etapa del trámite legislativo se prefirió no innovar en esta materia. Ello podría implicar una restricción en la contratación y una perturbación en los intereses del Estado.

Remarcó que una norma que puede estar bien inspirada puede generar efectos indeseados en términos de bien común.

El Presidente de la Comisión, Honorable Senador señor Harboe no compartió lo señalado precedentemente.

Destacó que las normas bien inspiradas tienen efectos cuando el regulado no adopta las medidas pertinentes para evitar caer en la conducta que le importa una determinada sanción.

Manifestó que debe instaurarse una cultura de respeto de las relaciones laborales. La creación de la cultura de protección de datos personales se construiría sobre la base de una potencial sanción, a saber, no contratar con el principal proveedor de servicios que es el Estado.

Ello constituye un incentivo positivo para que las empresas adopten mecanismos preventivos.

Concluido el debate sobre este artículo, la Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó con enmiendas formales esta disposición.

Artículo 44

En seguida, la Comisión estudió el artículo 44 del proyecto de ley del Ejecutivo que establece las reglas sobre la prescripción de las infracciones. Su texto es el siguiente:

“Artículo 44.- Prescripción. Las infracciones previstas en esta ley prescriben en el plazo de tres años, contado desde la ocurrencia del hecho que originó la infracción.

En caso de infracciones continuadas, el plazo de prescripción se contará desde el día en que la infracción haya cesado.

Se interrumpe la prescripción con la notificación del inicio del procedimiento administrativo correspondiente.

Las sanciones que se impongan por una infracción a la presente ley prescriben en el plazo **de dos años**, contados desde la fecha en que la resolución que impone la sanción quede ejecutoriada.

Las acciones establecidas en esta ley prescribirán en el plazo de tres años.

Las acciones civiles que deriven de una infracción a la presente ley prescribirán en el plazo de tres años, contado desde que se encuentre ejecutoriada la resolución administrativa o la sentencia judicial, según sea el caso, que imponga la multa respectiva.”.

Durante el examen de este precepto, se tuvo presente lo que dispone el artículo 42 de la moción que se refunde en este informe. Dicha disposición establece que 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.

Al inicio del estudio de estas normas, **los representantes del Ejecutivo, señora Piedrabuena y señor Godoy**, propusieron a la Comisión aprobar el artículo del proyecto de ley del Gobierno, cambiando el inciso cuarto por el siguiente:

“Las sanciones que se impongan por una infracción a la presente ley prescriben en el plazo de **tres años**, contados desde la fecha en que la resolución que impone la sanción quede ejecutoriada.”.

El asesor del Ministerio de Hacienda, señor Godoy, explicó que en el texto refundido se realizó una innovación respecto a la propuesta original del Ejecutivo. Añadió que en el mencionado texto se propone uniformar los plazos de prescripción en tres años.

Consignó que las infracciones, el cobro eventual de la multa y la persecución de las acciones se deben realizar antes del cumplimiento del plazo ya mencionado.

Expresó que la norma establece una regla respecto al ejercicio de las acciones civiles, en términos que ésta solo se pueda interponer una vez resuelto el procedimiento administrativo que establece el hecho infraccional. Recalcó que la responsabilidad civil se origina a partir de la resolución administrativa o judicial, en el caso que haya reclamación que establezca la infracción.

El Presidente de la Comisión, Honorable Senador señor Harboe subrayó que lo que prescriben son las acciones para perseguir las infracciones.

Sugirió la siguiente redacción para los incisos primero y segundo:

“Artículo 44.- Prescripción. Las acciones para perseguir las infracciones previstas en esta ley prescriben en el plazo de tres años, contado desde la ocurrencia del hecho que originó la infracción.

En caso de infracciones continuadas, el plazo de prescripción de las referidas acciones, se contará desde el día en que la infracción haya cesado.”

El asesor del Comité Udi, señor Mery, indicó que el Ejecutivo ha puntualizado que el inicio del transcurso del plazo no es desde la perpetración del hecho ilícito, sino de un hecho posterior, y que la fuente de la responsabilidad, más que la conducta ilícita, sería un acto de la Administración. Atendido lo anterior, el plazo señalado sería superior a tres años.

El asesor del Ministerio de Hacienda, señor Godoy, constató que los hechos que originan la responsabilidad civil deben quedar determinados en el procedimiento infraccional. Estimó conveniente que las acciones civiles solo se puedan deducir una vez que la autoridad administrativa determine que la infracción se cometió. Agregó que en una norma posterior se determinó que las acciones civiles para perseguir la indemnización de perjuicio se tramitarán de acuerdo a las normas del juicio sumario, como una forma de acortar el procedimiento.

El asesor del Comité Udi, señor Mery, propuso que el plazo se suspenda mientras no se encuentre firma la resolución.

El Honorable Senador señor Araya sugirió elaborar una norma de clausura que señale que en el juicio civil no se puede volver a discutir los hechos, sino que solo el monto de los perjuicios.

El Presidente de la Comisión, Honorable Senador señor Harboe hizo presente que además de estas normas se deben observar los preceptos sobre responsabilidad civil consagrados en el Código Civil.

Concluido el debate sobre este precepto, el señor Presidente de la Comisión sometió a votación la siguiente redacción:

"Artículo 44.- Prescripción. Las acciones para perseguir la responsabilidad por las infracciones previstas en esta ley prescriben en el plazo de tres años, contado desde la ocurrencia del hecho que originó la infracción.

En caso de infracciones continuadas, el plazo de prescripción de las referidas acciones se contará desde el día en que la infracción haya cesado.

Se interrumpe la prescripción con la notificación del inicio del procedimiento administrativo correspondiente.

Las sanciones que se impongan por una infracción a la presente ley prescriben en el plazo de tres años, contados desde la fecha en que la resolución que impone la sanción quede ejecutoriada.

Las acciones civiles que deriven de una infracción a la presente ley prescribirán en el plazo de tres años, contado desde que se encuentre ejecutoriada la resolución administrativa o la sentencia judicial, según sea el caso, que imponga la multa respectiva.".

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó esta redacción para el artículo 44.

En una sesión posterior, los representantes del Ejecutivo sugirieron a la Comisión incorporar el inciso final del artículo 44, como nuevo inciso final del artículo 51.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, De Urresti y Harboe, aprobó la modificación propuesta por el Ejecutivo.

Artículo 45

A continuación, la Comisión trató el artículo 45 del proyecto de ley del Ejecutivo. Esta disposición, que encabeza un párrafo segundo, referido a los procedimientos administrativos, regula los procedimientos de tutela de derecho. Su texto es el siguiente:

"Artículo 45.- Procedimiento administrativo de tutela de derechos. El titular de datos podrá reclamar ante la Agencia de Protección de Datos Personales cuando el responsable le haya denegado, en forma expresa o tácita, una solicitud en que ejerce cualquiera de los derechos que le reconoce esta ley.

La reclamación presentada se tramitará conforme a las siguientes reglas:

a) Deberá ser presentada por escrito, dentro del plazo de 10 días contado desde que reciba la respuesta negativa del responsable de datos o haya vencido el plazo que disponía el responsable para responder el requerimiento formulado por el titular. La reclamación deberá señalar la decisión impugnada, acompañar todos los antecedentes en que se funda e indicar una dirección de correo electrónico donde se practicarán las notificaciones.

b) Recibido el reclamo, la Agencia de Protección de Datos Personales, dentro de los 3 días siguientes, deberá determinar si éste cumple con los requisitos establecidos en la letra anterior para ser acogido a tramitación. La resolución de la Agencia de Protección de Datos Personales que no acoja a trámite la reclamación deberá ser fundada y se notificará al titular.

c) Acogido el reclamo a tramitación, la Agencia de Protección de Datos Personales notificará al responsable de datos, quien dispondrá de un plazo de 10 días para responder la reclamación, acompañando todos los antecedentes que estime pertinentes. Las notificaciones que se practiquen al responsable se realizarán a la dirección de correo electrónico a que alude la letra c) del artículo 14 ter.

d) Vencido este plazo, haya o no contestado el responsable de los datos, y sólo si existen hechos sustanciales, pertinentes y controvertidos, se abrirá un término probatorio de 7 días en el cual las partes pueden hacer valer todos los medios de prueba que estimen convenientes.

e) El responsable de datos en su respuesta podrá allanarse a la reclamación, en cuyo caso deberá acompañar los antecedentes o testimonios que acrediten esta circunstancia. Verificado lo anterior y notificado el titular de datos, la Agencia de Protección de Datos

Personales procederá al archivo de los antecedentes, previa aplicación de la sanción, cuando correspondiere.

f) La Agencia de Protección de Datos Personales tendrá amplias facultades para solicitar antecedentes o informes que contribuyan a su resolución. Puede, asimismo, instar a las partes a alcanzar un acuerdo. Logrado un acuerdo, se archivarán los antecedentes.

g) La resolución del reclamo debe dictarse por la Agencia de Protección de Datos Personales dentro del plazo de 10 días desde recibida la respuesta del responsable de datos o desde el vencimiento de este plazo en caso que no haya respondido, o desde el término del período probatorio, según corresponda. La resolución que resuelva el reclamo deberá ser fundada.

h) En contra de esta resolución sólo procede el recurso de reposición, el que deberá ser interpuesto dentro del plazo de 5 días contado desde su notificación. La resolución que resuelva el recurso de reposición debe dictarse en el plazo de 5 días y será reclamable judicialmente dentro del plazo de 15 días, a través del procedimiento establecido en el artículo 47.

i) La interposición del reclamo administrativo suspende las operaciones de tratamiento o cesión de los datos personales que son objeto de la reclamación.

En todo lo no previsto en este artículo se aplicarán supletoriamente y en lo que corresponda las normas de la ley Nº 19.880.”.

Al iniciarse el estudio de esta materia, **los representantes del Ejecutivo** sugirieron a la Comisión aprobar el texto del artículo antes descrito, con algunos cambios, especialmente en los plazos que originalmente estaban considerados. Su texto es el siguiente:

“Artículo 45.- Procedimiento administrativo de tutela de derechos. El titular de datos podrá reclamar ante la Agencia de Protección de Datos Personales, cuando el responsable le haya denegado, en forma expresa o tácita, una solicitud en que ejerce cualquiera de los derechos que le reconoce esta ley.

La reclamación presentada se tramitará conforme a las siguientes reglas:

a) Deberá ser presentada por escrito, dentro del plazo de **15 días** contado desde que reciba la respuesta negativa del responsable de datos o haya vencido el plazo que disponía el responsable para responder el requerimiento formulado por el titular. La reclamación

deberá señalar la decisión impugnada, acompañar todos los antecedentes en que se funda e indicar una dirección de correo electrónico donde se practicarán las notificaciones.

b) Recibido el reclamo, la Agencia de Protección de Datos Personales, dentro de los **10 días** siguientes, deberá determinar si éste cumple con los requisitos establecidos en la letra anterior para ser acogido a tramitación. En caso de que no se acoja a trámite la reclamación, la resolución de la Agencia de Protección de Datos Personales debe ser fundada y se notificará al titular.

c) Acogido el reclamo a tramitación, la Agencia de Protección de Datos Personales notificará al responsable de datos, quien dispondrá de un plazo de **15 días** para responder la reclamación, acompañando todos los antecedentes que estime pertinentes. Las notificaciones que se practiquen al responsable se realizarán a la dirección de correo electrónico a que alude la letra c) del artículo 14 ter.

d) Vencido este plazo, haya o no contestado el responsable de los datos y, sólo si existen hechos sustanciales, pertinentes y controvertidos, se abrirá un término probatorio de **10 días** en el cual las partes pueden hacer valer todos los medios de prueba que estimen convenientes.

e) El responsable de datos en su respuesta podrá allanarse a la reclamación, en cuyo caso deberá acompañar los antecedentes o testimonios que acrediten esta circunstancia. Verificado lo anterior y notificado el titular de datos, la Agencia de Protección de Datos Personales procederá al archivo de los antecedentes, previa aplicación de la sanción, cuando correspondiere.

f) La Agencia de Protección de Datos Personales tendrá amplias facultades para solicitar antecedentes o informes que contribuyan a su resolución. Además, podrá instar a las partes a alcanzar un acuerdo. Logrado un acuerdo, se archivarán los antecedentes.

g) La resolución del reclamo deberá dictarse por la Agencia de Protección de Datos Personales y deberá ser fundada. El procedimiento administrativo de tutela de derechos no podrá superar los seis meses.

h) La resolución de la Agencia de Protección de Datos Personales será reclamable judicialmente dentro del plazo de 15 días, a través del procedimiento establecido en el artículo 47.

i) Junto con la interposición del reclamo, a petición fundada del titular y sólo en casos justificados, la Agencia de

Protección de Datos Personales podrá suspender el tratamiento de los datos personales que conciernen al titular y que son objeto de la reclamación, debiendo previamente oír al responsable de datos.

Las reclamaciones y las solicitudes de suspensión del tratamiento formuladas en caso de rechazo de una solicitud de bloqueo temporal, deberán ser resueltas por la Agencia de Protección de Datos Personales en el más breve plazo, sin necesidad de oír previamente a las partes.”.

Al explicar este procedimiento, **el asesor del Ministerio de Hacienda, señor Godoy,** indicó que el procedimiento que se plantea es relevante, para que los titulares de datos puedan ejercer sus derechos en el evento que los responsables no cumplan con las obligaciones que establece la ley.

Para tal efecto se crean en sede administrativa dos procedimientos. El primero de ellos corresponde al de tutela de derechos que está fundamentalmente orientado a que las personas, una vez que ejercen algunos de los derechos que reconoce el presente cuerpo legal puedan recurrir a la Agencia, en el evento que el responsable no responde a una solicitud o lo haga negativamente. Observó que el objetivo de dicho procedimiento es que se otorgue tutela del derecho que invoque el titular.

Mencionó que el segundo procedimiento, por infracción de ley, se regula en el artículo siguiente.

El Honorable Senador señor Araya solicitó que, atendidas las últimas sentencias del Tribunal Constitucional, el Ejecutivo explique la atribución consagrada en la letra f), del artículo en estudio.

Recomendó, en esa misma letra, incorporar una norma de clausura que disponga que las opiniones emitidas por la Agencia al momento en que insta que las partes a que logren un acuerdo, no la inhabilitarán respecto de la resolución final.

El Presidente de la Comisión, Honorable Senador señor Harboe, expresó que en la letra b) se señala que cuando la Agencia no admite a tramitación el recurso, la resolución de ésta, debe ser fundada y notificada. Preguntó si ella es apelable.

El asesor del Ministerio de Hacienda, señor Godoy, consignó que es apelable tanto la resolución de término del reclamo, como aquella que deniega la solicitud.

Hizo presente que en el artículo 47 que se examinará más adelante, esta iniciativa dispone lo siguiente:

“Las personas naturales o jurídicas que se vean afectadas o agraviadas por una resolución final o de término de la Agencia de Protección de Datos Personales podrán deducir un reclamo de ilegalidad ante la Corte de Apelaciones de Santiago o la del lugar donde se encuentre domiciliado el reclamante, a elección de este último.”

El Presidente de la Comisión, Honorable Senador señor Harboe, sugirió incorporar en la letra h), a ambas resoluciones, porque puede entenderse que la mencionada letra solo se refiera a la resolución de término. Es decir, aquella en que la Agencia analice el fondo.

El asesor del Ministerio de Hacienda, señor Godoy, estimó que se debe considerar agregar una norma de clausura, de acuerdo a lo propuesto por el Honorable Senador, señor Araya.

Recordó que el procedimiento en estudio no busca sancionar infracciones, sino que intenta proteger el derecho del titular en términos de hacer efectivo, por la vía administrativa o judicial, el ejercicio de los derechos que le reconoce la ley. Por lo tanto, precisó que si durante un procedimiento administrativo se resuelve el interés en favor del titular, se entiende que está satisfecho el objetivo para el cual se generó el procedimiento.

El asesor del Honorable Senador Larraín, señor Olmedo, recomendó que en la letra d), se faculte a la Agencia para que decida abrir un término probatorio. Enfatizó que no es conveniente que sea imperativa la apertura de éste.

Propuso que si la Agencia estima necesario escuchar a las partes, éstas sean citadas a una audiencia.

El Presidente de la Comisión, Honorable Senador señor Harboe, manifestó que esto último resulta más adecuado incorporarlo en el procedimiento infraccional.

El asesor del Honorable Senador Larraín, señor Olmedo, consideró pertinente considerarlo en ambos procedimientos.

El asesor del Comité Udi, señor Mery, consultó si puede ejercer la acción solo el titular de derechos.

Constató que el plazo de 15 días de la letra a), constituye una remisión a los términos consagrados en la ley N° 19.880, que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado.

Mostró su inquietud respecto al plazo establecido en la letra g), donde se señala que el procedimiento administrativo de tutela de derechos no podrá superar los seis meses.

Respecto a la observación planteada por el asesor, señor Olmedo, **el Honorable Senador señor Araya** ratificó que la letra d) es clara en su redacción al disponer que solo si existen hechos sustanciales, pertinentes y controvertidos, se abrirá un término probatorio de 10 días.

Sostuvo que la posibilidad de que la Agencia cite a las partes a una audiencia puede incorporarse en la letra f).

El asesor del Ministerio de Hacienda, señor Godoy aseveró que puede modificarse la letra d) y otorgarle a la Agencia la facultad de abrir el término probatorio.

Añadió que se persigue que el procedimiento sea expedito. Pese a ello, destacó que se puede incorporar la opción de que la Agencia cite a las partes a una audiencia.

Afirmó que está de acuerdo en que se agregue la norma de clausura propuesta por el Honorable Senador señor Araya.

Se mostró partidario de conservar la norma que señala que el procedimiento administrativo de tutela de derechos no podrá superar los seis meses.

El asesor del Honorable Senador Larraín, señor Olmedo, ratificó que este último plazo se encuentra consagrado en la ley N° 20.285, sobre acceso a la información pública, en un procedimiento similar sobre protección de amparo. Manifestó que dicho término ha constituido un estímulo importante para el constante perfeccionamiento de los procesos internos de seguimiento de casos.

El asesor del Ministerio de Hacienda, señor Godoy, recalcó que el plazo mencionado permite alinear los incentivos dentro de la organización.

El Presidente de la Comisión, Honorable Senador señor Harboe, recomendó que se haga referencia a la ley N° 19.880, en relación a las normas de carácter jurisdiccional.

El asesor del Honorable Senador Larraín, señor Olmedo, aseveró que una similar discusión se produjo en la Ley de Acceso a la Información Pública. Agregó que el Consejo para la Transparencia decidió,

después de un par de años, no remitirse a la ley N° 19.880, porque la cantidad de recursos que dicho cuerpo legal confiere, produjo una dilación de los procedimientos ante el mencionado Consejo. Lo anterior atentaba en contra de la efectiva y pronta tutela.

Es por ello que el Consejo, en virtud de un acuerdo general, decidió regirse exclusivamente por las normas procedimentales establecidas en la ley N° 20.285, sobre acceso a la información pública.

Finalmente, **el Presidente de la Comisión, Honorable Senador señor Harboe**, declaró cerrado el debate, y puso en votación el artículo 45.

La Comisión por la unanimidad de sus integrantes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó este artículo, con la enmienda de sustituir en la letra d) la expresión "se abrirá" por "se podrá abrir".

En una sesión posterior, el Ejecutivo propuso una indicación a la Comisión para reemplazar las letras f) y h), por las siguientes:

- "f) La Agencia de Protección de Datos Personales tendrá amplias facultades para solicitar antecedentes o informes que contribuyan a su resolución. Podrá convocar a las partes a una audiencia e instarlas a alcanzar un acuerdo. Las opiniones que puedan expresar los funcionarios de la Agencia de Protección de Datos Personales en esta audiencia, no los inhabilitará para seguir conociendo del asunto en caso que no se alcance un acuerdo. Logrado el acuerdo, se archivarán los antecedentes."

El asesor del Comité Udi, señor Mery, en relación a la frase: "Las opiniones que puedan expresar los funcionarios de la Agencia de Protección de Datos Personales en esta audiencia, no los inhabilitará para seguir conociendo del asunto en caso que no se alcance un acuerdo.", constató que el único que tiene la potestad resolutiva es el Director.

El Presidente de la Comisión, Honorable Senador señor Harboe, consignó que el sentido de esta disposición es evitar que en el marco de un proceso administrativo, las opiniones vertidas por los funcionarios los inhabiliten en un procedimiento posterior.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, De Urresti y Harboe, aprobó la modificación propuesta por el Ejecutivo.

- “h) La resolución de la Agencia de Protección de Datos Personales que no acoge a tramitación un reclamo y la resolución que resuelve la reclamación, podrán ser impugnadas judicialmente dentro del plazo de 15 días contados desde su notificación, a través del procedimiento establecido en el artículo 47.”

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, De Urresti y Harboe, aprobó la modificación propuesta por el Ejecutivo.

El texto acordado precedentemente fue ratificado mediante una indicación que presentó el Ejecutivo, la que se dio por aprobada con las votaciones señaladas precedentemente.

Artículo 46

A continuación, la Comisión trató el artículo 46 del proyecto de ley del Ejecutivo que incorpora a la ley N° 19.628 una disposición que regula el procedimiento administrativo por infracción de ley. Su texto es el siguiente:

“Artículo 46.- Procedimiento administrativo por infracción de ley. El procedimiento sancionatorio por las infracciones que cometan los responsables de datos por incumplimiento o vulneración de los principios y obligaciones establecidas en esta ley será instruido por la Agencia de Protección de Datos Personales conforme a las siguientes reglas:

a) La Agencia de Protección de Datos Personales podrá iniciar un procedimiento sancionatorio de oficio, a petición de parte, como resultado de un proceso de fiscalización o a consecuencia de una reclamación presentada por un titular de datos en virtud del procedimiento establecido en el artículo 45 de esta ley.

b) La Agencia de Protección de Datos Personales deberá presentar una formulación de cargos en contra del responsable de datos en que describa los hechos que configuran la infracción, los principios y obligaciones incumplidos o vulnerados por el responsable, las normas legales infringidas y cualquier otro antecedente que sirva para sustentar la formulación.

c) La formulación de cargos debe notificarse al responsable de datos a la dirección de correo electrónico señalada en la letra c) del artículo 14 ter.

d) El responsable de datos tiene un plazo de 10 días para presentar sus descargos. En esa oportunidad el responsable de datos puede acompañar todos los antecedentes que estime pertinente para desacreditar los hechos imputados. Junto con los descargos, el responsable podrá fijar una dirección de correo electrónico distinta a la señalada en la letra c) del artículo 14 para la realización de las demás comunicaciones y notificaciones.

e) Recibidos los descargos o transcurrido el plazo otorgado para ello, la Agencia de Protección de Datos Personales podrá abrir un término probatorio de 7 días, en el caso que existan hechos sustanciales, pertinentes y controvertidos.

f) La Agencia de Protección de Datos Personales dará lugar a las medidas o diligencias probatorias que solicite el responsable en sus descargos, siempre que sean pertinentes y necesarias. En caso de rechazo, deberá fundar su resolución.

g) Los hechos investigados y las responsabilidades de los presuntos infractores pueden acreditarse mediante cualquier medio de prueba admisible en derecho, los que se apreciarán de acuerdo a las reglas de la sana crítica.

h) La Agencia de Protección de Datos Personales tendrá amplias facultades para solicitar antecedentes o informes que contribuyan a su resolución.

i) La resolución que ponga fin al procedimiento sancionatorio debe ser fundada y resolver todas las cuestiones planteadas en el expediente, pronunciándose sobre cada una de las alegaciones y defensas formuladas por el responsable de datos, y contendrá la declaración de haberse configurado el incumplimiento o vulneración de los principios y obligaciones establecidos en la ley por el responsable o su absolución, según corresponda. En caso que la Agencia de Protección de Datos Personales considere que se ha verificado la infracción, en la misma resolución ponderará las circunstancias que agravan o atenúan la responsabilidad del infractor e impondrá la sanción, de acuerdo a la gravedad de la infracción cometida. Esta resolución debe dictarse dentro de los 20 días siguientes de recibidos los descargos, o desde el vencimiento de este plazo, en caso que el responsable no haya respondido, o desde el término del probatorio, según corresponda.

j) La resolución que establezca el incumplimiento o vulneración a los principios y obligaciones de esta ley y aplique la sanción correspondiente debe ser fundada. Esta resolución debe indicar también los recursos administrativos y judiciales que procedan contra ella en conformidad

a esta ley, los órganos ante los que deben presentarse y el plazo para su interposición.

k) En contra de esta resolución sólo procede el recurso de reposición que debe ser interpuesto dentro del plazo de 5 días, contado desde la notificación respectiva. La resolución que resuelva el recurso de reposición debe dictarse en el plazo de 10 días y será reclamable judicialmente conforme al artículo siguiente.

En todo lo no previsto en este artículo se aplicarán supletoriamente y en lo que corresponda, las normas de la ley Nº 19.880.”.

Al iniciarse el estudio de esta disposición, **los representantes del Ejecutivo, señora Piedrabuena y señor Godoy**, sugirieron a la Comisión aprobar este artículo del proyecto de ley del Ejecutivo, enmendado en los siguientes términos.

“Artículo 46.- Procedimiento administrativo por infracción de ley. La determinación de las infracciones que cometan los responsables de datos por incumplimiento o vulneración de los principios, derechos y obligaciones establecidas en esta ley y la aplicación de las sanciones correspondientes, se sujetará a las siguientes reglas especiales:

a) El procedimiento sancionatorio será instruido por la Agencia de Protección de Datos Personales.

b) La Agencia de Protección de Datos Personales podrá iniciar un procedimiento sancionatorio de oficio o a petición de parte, como resultado de un proceso de fiscalización o a consecuencia de una reclamación presentada por un titular de datos en virtud del procedimiento establecido en los artículos 23 y 45 de esta ley.

c) La Agencia de Protección de Datos Personales deberá presentar una formulación de cargos en contra del responsable de datos en que describa los hechos que configuran la infracción, los principios y obligaciones incumplidos o vulnerados por el responsable, las normas legales infringidas y cualquier otro antecedente que sirva para sustentar la formulación.

d) La formulación de cargos debe notificarse al responsable de datos a la dirección de correo electrónico señalada en la letra c) del artículo 14 ter.

e) El responsable de datos tendrá un plazo de 15 días para presentar sus descargos. En esa oportunidad el responsable de datos puede acompañar todos los antecedentes que estime pertinente para desacreditar los hechos imputados. Junto con los descargos, el responsable

deberá fijar una dirección de correo electrónico a través de la cual se realizarán todas las demás comunicaciones y notificaciones.

f) Recibidos los descargos o transcurrido el plazo otorgado para ello, la Agencia de Protección de Datos Personales podrá abrir un término probatorio de 10 días, en el caso que existan hechos sustanciales, pertinentes y controvertidos.

g) La Agencia de Protección de Datos Personales dará lugar a las medidas o diligencias probatorias que solicite el responsable en sus descargos, siempre que sean pertinentes y necesarias. En caso de rechazo, deberá fundar su resolución.

h) Los hechos investigados y las responsabilidades de los presuntos infractores pueden acreditarse mediante cualquier medio de prueba admisible en derecho, los que se apreciarán de acuerdo a las reglas de la sana crítica.

i) La Agencia de Protección de Datos Personales tendrá amplias facultades para solicitar antecedentes o informes que contribuyan a su resolución.

j) La resolución que ponga fin al procedimiento sancionatorio debe ser fundada y resolver todas las cuestiones planteadas en el expediente, pronunciándose sobre cada una de las alegaciones y defensas formuladas por el responsable de datos y, contendrá la declaración de haberse configurado el incumplimiento o vulneración de los principios, derechos y obligaciones establecidos en la ley por el responsable o su absolución, según corresponda. En caso que la Agencia de Protección de Datos Personales considere que se ha verificado la infracción, en la misma resolución ponderará las circunstancias que agravan o atenúan la responsabilidad del infractor e impondrá la sanción, de acuerdo a la gravedad de la infracción cometida.

k) La resolución que establezca el incumplimiento o vulneración a los principios, derechos y obligaciones de esta ley, y aplique la sanción correspondiente, deberá ser fundada. Esta resolución debe indicar los recursos administrativos y judiciales que procedan contra ella en conformidad a esta ley, los órganos ante los que deben presentarse y los plazos para su interposición.

l) En contra de esta resolución procederá el recurso de reposición que deberá ser interpuesto dentro del plazo de 5 días, contados desde la notificación respectiva. La resolución que resuelva el recurso de reposición debe dictarse en el plazo de 15 días y será reclamable judicialmente conforme al artículo siguiente.

El procedimiento administrativo de infracción de ley no podrá superar los seis meses.”.

Al explicar esta nueva redacción, **el asesor del Ministerio de Hacienda, señor Godoy,** manifestó que en ella se uniforma el procedimiento para los agentes privados y para los públicos. Por lo tanto, el procedimiento de infracción de ley rige para ambos.

Desde el punto de vista del procedimiento, expresó que se busca eliminar o reducir cualquier atisbo de eventual discrecionalidad en la facultad investigadora y sancionadora de la Agencia. Agregó que desde esa perspectiva se establecen con bastante rigor los pasos que se deben dar durante el procedimiento de investigación de una infracción administrativa y en la aplicación de las sanciones.

Finalmente, destacó que la norma en discusión fue revisada, tomando en consideración el informe elaborado por la Exma. Corte Suprema.

El Honorable Senador señor Larraín apuntó que surge inevitablemente la pregunta de hasta dónde llega la potestad sancionatoria de organismos administrativos.

Llamó la atención que se está yendo más allá del ámbito propio de infracciones administrativas que nuestro ordenamiento reconoce a este tipo de organismos.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena aseveró que este tipo de atribuciones está presente en otros organismos fiscalizadores del sector público. Afirmó que, por ejemplo, la Comisión para el Mercado Financiero cuenta con un procedimiento sancionatorio.

Seguidamente, **el Honorable Senador señor Larraín** consultó si se justifica el recurso de reposición consagrado en la letra l).

El asesor del Ministerio de Hacienda, señor Godoy, subrayó que el mencionado recurso busca evitar abrir la sede judicial.

El Presidente de la Comisión, Honorable Senador señor Harboe precisó que en el fallo del Tribunal Constitucional, sobre la Superintendencia de Bancos con Corpbanca, se reconoce el principio de deferencia técnica. Agregó que, asimismo, se exige que haya habido debido proceso.

Atendido lo anterior, y en relación al artículo en estudio, no advierte mayor complicación desde el punto de vista constitucional. Recalcó que respecto a la presente iniciativa, se reúnen los requisitos de que existe una autoridad técnica y se consagra un debido proceso.

El asesor del Comité Udi, señor Mery, hizo presente que la Agencia es un organismo que puede tener muchos funcionarios, y no será ésta la que sustanciará el proceso y al mismo tiempo lo resolverá. Sugirió para dividir la función instructora de la de resolución, adoptar el criterio que se sigue en el artículo 61 de la ley N° 20.529 que crea el sistema nacional de aseguramiento de la calidad de la educación parvularia, básica y media y su fiscalización.

El mencionado artículo dispone lo siguiente:

“Artículo 61.- Admitida una denuncia o reclamo a tramitación, el Director Regional ordenará la apertura de un expediente y designará al funcionario encargado de su tramitación, quien notificará al denunciado o reclamado.”

Recalcó que debe existir una división entre el funcionario encargado de la tramitación y aquel que debe resolver el reclamo.

Sugirió que en el encabezado de la letra c) se anteponga una redacción similar a la del artículo 61 antes transcrito.

El asesor del Ministerio de Hacienda, señor Godoy, consignó que la Agencia es una institución que carece de una expresión territorial. Enfatizó que el único cargo que se crea es el del Director. Agregó que en ella se establece una dotación que se incrementará en el tiempo.

Connotó que se puede establecer que funcionarios bajo la dependencia del Director instruyan los procedimientos y sea éste último quien ejerza la facultad de aplicar la sanción.

El Presidente de la Comisión, Honorable Senador señor Harboe sugirió aprobar el artículo en estudio, sin perjuicio que el Ejecutivo pueda, posteriormente, formular proposiciones para acoger las observaciones formuladas precedentemente.

El Honorable Senador señor Araya sugirió, además, precisar en la redacción de la letra l), que se puede interponer el recurso de apelación, independiente de la presentación de la reposición.

Finalmente, **el Presidente de la Comisión, Honorable Senador señor Harboe** declaró cerrado el debate, y puso en votación el artículo 46.

La Comisión aprobó, por mayoría de votos, el artículo 46 con las enmiendas sugeridas por los representantes del Ejecutivo. Se pronunciaron a favor los Honorables Senadores señores Araya y Harboe. Se abstuvo el Honorable Senador señor Larraín.

En una sesión posterior, el Ejecutivo sugirió a la Comisión aprobar las siguientes enmiendas a las letras b), k) y l), del artículo 46:

En la letra b) ya aprobada, agregar antes del punto aparte, lo siguiente: “, en este último caso, deberá certificar la recepción del reclamo. Junto con la apertura del expediente, la Agencia de Protección de Datos Personales deberá designar un funcionario responsable de la instrucción del procedimiento.”

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, De Urresti y Harboe, aprobó la modificación propuesta por el Ejecutivo.

En la letra k) ya aprobada, agregar en su parte final la siguiente frase: “La resolución de la Agencia de Protección de Datos Personales que resuelve el procedimiento por infracción de ley será reclamable judicialmente conforme al artículo siguiente.”

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, De Urresti y Harboe, aprobó la modificación propuesta por el Ejecutivo.

Finalmente, el Ejecutivo propuso reemplazar la letra l) y el inciso final del artículo 46 por el siguiente:

“l) El procedimiento administrativo de infracción de ley no podrá superar los seis meses. Cuando hayan transcurrido más de seis meses desde la fecha de la certificación indicada en la letra b) de este artículo sin que la Agencia de Protección de Datos Personales haya resuelto la reclamación, el titular podrá presentar un reclamo de ilegalidad en los términos previstos en el siguiente artículo.”

El asesor del Honorable Senador Larraín, señor Olmedo hizo presente que se debiese contemplar la posibilidad de que el infractor pueda presentar un reclamo.

El asesor del Comité Udi, señor Mery sugirió que la prerrogativa se establezca respecto de ambos.

Propuso reemplazar el término “el titular”, por “el interesado”. Explicó que ante la falta de resolución, no se debe circunscribir el reclamo únicamente al titular.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, De Urresti, Harboe y Larraín, aprobó, con esta última enmienda, la nueva letra l) propuesta por el Ejecutivo.

El texto acordado precedentemente fue ratificado mediante una indicación que presentó el Ejecutivo, la que se dio por aprobada con las votaciones señaladas precedentemente.

Artículo 47

Seguidamente, la Comisión consideró el artículo 47 del proyecto de ley del Ejecutivo que establece las reglas del procedimiento de reclamación judicial. Su texto es el siguiente:

“Artículo 47.- Reclamación judicial. Las personas naturales o jurídicas que se vean afectadas por una resolución final o de término de la Agencia de Protección de Datos Personales podrán deducir un reclamo de ilegalidad ante la Corte de Apelaciones de Santiago o la del lugar donde se encuentre domiciliado el reclamante, a elección de este último. El reclamo deberá interponerse dentro de los 15 días siguientes a la notificación de la resolución impugnada, según las siguientes reglas:

a) El reclamante señalará en su escrito, con precisión, la resolución objeto del reclamo, la o las normas legales que se suponen infringidas, la forma en que se ha producido la infracción y, cuando procediere, las razones por las cuales el acto le perjudica. Si la reclamación no cumple con estos requisitos, la Corte podrá declararla inadmisible.

b) El titular de datos o el responsable de los mismos, según corresponda, podrá hacerse parte en el respectivo reclamo de conformidad a las normas generales.

c) La Corte podrá decretar orden de no innovar cuando la ejecución del acto impugnado produzca un daño irreparable al recurrente.

d) Recibida la reclamación, la Corte requerirá de informe a la Agencia de Protección de Datos Personales, concediéndole un plazo de diez días al efecto.

e) Evacuado el traslado o teniéndosele por evacuado en rebeldía, la Corte podrá abrir un término de prueba, si así lo estima necesario, el que se regirá por las reglas de los incidentes que contempla el Código de Procedimiento Civil.

f) Vencido el término de prueba, se ordenará traer los autos en relación. La vista de esta causa gozará de preferencia para su inclusión en la tabla.

g) Si la Corte da lugar al reclamo en su sentencia decidirá u ordenará, según sea procedente, la rectificación del acto impugnado y la dictación de la respectiva resolución, según corresponda.

h) Tratándose de reclamaciones en contra de una resolución que resuelve un procedimiento sancionatorio, la Corte podrá confirmar o revocar la resolución impugnada, establecer o desechar la comisión de la infracción, según corresponda y, mantener, dejar sin efecto o modificar la sanción impuesta al responsable.

i) En todo aquello no regulado por el presente artículo, regirán las normas establecidas en el Código Orgánico de Tribunales y en el Código de Procedimiento Civil, según corresponda.”.

Al iniciarse el debate de esta disposición, **los representantes del Ejecutivo, señora Piedrabuena y señor Godoy**, sugirieron a la Comisión aprobar este precepto del proyecto de ley del Gobierno, enmendado en los siguientes términos:

“Artículo 47.- Procedimiento de reclamación judicial. Las personas naturales o jurídicas que se vean afectadas **o agraviadas** por una resolución final o de término de la Agencia de Protección de Datos Personales podrán deducir un reclamo de ilegalidad ante la Corte de Apelaciones de Santiago o la del lugar donde se encuentre domiciliado el reclamante, a elección de este último. El reclamo deberá interponerse dentro de los 15 días siguientes a la notificación de la resolución impugnada, según las siguientes reglas:

a) El reclamante señalará en su escrito, con precisión, la resolución objeto del reclamo, la o las normas legales que se suponen infringidas, la forma en que se ha producido la infracción, y cuando procediere, las razones por las cuales el acto **le causa agravio**.

b) El titular de datos o el responsable de los mismos, según corresponda, podrá hacerse parte en el respectivo reclamo de conformidad a las normas generales.

c) La Corte podrá decretar orden de no innovar cuando la ejecución del acto impugnado le produzca un daño irreparable al recurrente. **Asimismo, podrá declarar inadmisible la reclamación si el escrito no cumple con las condiciones señaladas en la letra a) anterior.**

d) Recibida la reclamación, la Corte requerirá de informe a la Agencia de Protección de Datos Personales, concediéndole un plazo de diez días al efecto.

e) Evacuado el traslado o teniéndosele por evacuado en rebeldía, la Corte puede abrir un término de prueba, si así lo estima necesario, el que se regirá por las reglas de los incidentes que contempla el Código de Procedimiento Civil.

f) Vencido el término de prueba, se ordenará traer los autos en relación. La vista de esta causa gozará de preferencia para su inclusión en la tabla.

g) Si la Corte da lugar al reclamo, en su sentencia decidirá si existió agravio y ordenará, según sea procedente, la rectificación del acto impugnado y la dictación de la respectiva resolución, según corresponda.

h) Tratándose de reclamaciones en contra de una resolución que resuelve un procedimiento sancionatorio, la Corte podrá confirmar o revocar la resolución impugnada, establecer o desechar la comisión de la infracción, según corresponda y, mantener, dejar sin efecto o modificar la sanción impuesta al responsable.

i) En todo aquello no regulado por el presente artículo, regirán las normas establecidas en el Código Orgánico de Tribunales y en el Código de Procedimiento Civil, según corresponda.”.

Al iniciarse el estudio de este precepto se tuvo presente lo señalado por la Excma. Corte Suprema en su Oficio N° 63-2017, del 3 de mayo de 2017, en que señala lo siguiente:

“Que si bien en términos generales la norma propuesta se encuentra acorde con la ponencia de la Corte, pueden formularse algunas observaciones en pro de la coherencia del sistema que se plantea. Como sucede, por ejemplo, con el concepto de “perjuicio” que utiliza la norma, que genera ambigüedades, en el sentido de producir cuestionamientos como: ¿se requerirá de un perjuicio económico, claramente

identificable o bastará con acreditar un perjuicio de cualquier índole? ¿El concepto exigiría entonces, la acreditación de un perjuicio propiamente tal, o se refiere más a una especie de agravio? Esta última alternativa parece más acorde con las disposiciones procedimentales de la reclamación, que exigen identificar “las razones por las cuales el acto le perjudica”.

En tal sentido, cabe señalar que respecto a la información que el Estado puede restringir, la Corte Interamericana también se ha pronunciado, señalando una serie de estándares que pueden dar luces sobre el agravio exigible para dar paso a esta reclamación lo cual habrá de tenerse en cuenta al afinar la normativa de que se trata. Así lo ha manifestado en el caso Claude Reyes v. Chile.”.

Sobre esta observación, **el asesor del Ministerio de Hacienda, señor Godoy,** hizo presente que la nueva redacción sugerida por el Ejecutivo es posterior al informe de la Excma. Corte Suprema, y las observaciones formuladas por el Máximo Tribunal fueron recogidas en esta nueva disposición.

El Presidente de la Comisión, Honorable Senador señor Harboe, manifestó que el afectado recurrirá ante los tribunales de justicia cuando la resolución de la Agencia le sea desfavorable. En tal caso, los litigantes han de ser el afectado y el emisor de la resolución que se reclama, es decir, la Agencia.

Agregó que no ve razón para que en la letra b), se consigne la posibilidad de que el titular o responsable de datos pueda hacerse parte de este proceso, ya que esa discusión de fondo ya se produjo en la instancia administrativa. Constató que si le otorgamos la posibilidad al titular de datos que se haga parte de este reclamo judicial, estamos propiciando que el afectado tenga que litigar contra el responsable de datos y la Agencia.

El asesor del Ministerio de Hacienda, señor Godoy, sostuvo que se permite que el responsable se haga parte en este procedimiento, para que no se entienda que la Agencia representa a una de las partes. Esta última tiene que defender la legalidad del acto que dictó.

El Honorable Senador señor Larraín estimó que cuando se hacen reparos a la potestad sancionatoria de órganos administrativos, no es para evitar que no haya sanciones en los casos en que se transgredan las normas, sino que la pregunta que se debe responder es quién es la autoridad competente para imponer cierto tipo de sanciones. Observó que en lo fundamental es el Poder Judicial el llamado a resolver.

En relación a la norma, señaló entender lo expresado por el Presidente de la Comisión, Honorable Senador señor

Harboe. Sin embargo, consignó que lo que ocurre acá es similar a lo que sucede en el proceso penal, en que el fiscal no representa a las víctimas.

Enfatizó que la Agencia tendrá su punto de vista que puede no ser el mismo del titular. Se mostró partidario de no privar al responsable de datos del derecho de ser parte en el respectivo reclamo.

El Presidente de la Comisión, Honorable Senador señor Harboe, consideró que no es adecuada la analogía que se hace con el Ministerio Público, porque éste es parte interesada en el proceso. Destacó que la Agencia de Protección actúa como un órgano jurisdiccional administrativo.

Añadió que desde el punto de vista del procedimiento administrativo, existen dos partes, el afectado y el titular o responsable de datos. Constató que la controversia entre ellos, debe ser resuelta por la Agencia y el reclamo del afectado ante los tribunales de justicia surge de la resolución del mencionado órgano.

Resaltó que la instancia para que el titular ejerza su legítimo derecho, es ante la autoridad administrativa. Si el responsable de datos considera que la Agencia no falla adecuadamente, será él quien deberá recurrir ante los tribunales de justicia.

El asesor del Honorable Senador Larraín, señor Olmedo, comentó la experiencia del Consejo para la Transparencia respecto a este tema. Relató que hubo casos en que reclamado y reclamante recurrieron porque no quedaron satisfechos con la decisión del Consejo.

Expresó que se podrá deducir el reclamo de ilegalidad ante la Corte de Apelaciones de Santiago o la del lugar donde se encuentre domiciliado el reclamante, a elección de este último. Lo anterior obligará a la Agencia a generar una suerte de Defensoría en todas las Cortes de Apelaciones.

El asesor del Comité Udi, señor Mery, sugirió que en el inciso primero se reemplace: “Las personas naturales o jurídicas que se vean afectadas o agraviadas”, por: “Las personas agraviadas”. Propuso eliminar en la letra a) la expresión: “cuando procediere”. Recomendó invertir el orden de los párrafos en la letra c), porque la Corte en primer lugar declara la admisibilidad, y luego podrá decretar orden de no innovar.

Agregó que en la letra h) se menciona a la resolución que resuelve un procedimiento sancionatorio. Preguntó si ella comprende la que resuelve y la de término. Indicó que en la misma letra, se dispone que la Corte podrá confirmar o revocar la resolución impugnada, lo

que da a entender que no estamos ante una reclamación, sino ante una apelación, por el lenguaje utilizado.

Consultó si es recurrible la falta de resolución en el plazo de seis meses como una fórmula de rechazo ficto del reclamo.

El asesor del Ministerio de Hacienda, señor Godoy, aseveró que se puede establecer que transcurrido los seis meses se entienda rechazado el reclamo, en caso que éste no se haya resuelto.

Agregó que el procedimiento que se consagra, viene a reproducir el reclamo de ilegalidad que se establece en la Ley Orgánica Constitucional de Municipalidades.

Coincidió con la observación efectuada a la letra c).

Constató que el reclamo judicial se puede activar por el procedimiento de tutela y por la infracción a la ley. La letra g), viene a regular todas aquellas materias que no son procedimiento infraccional. La letra h) regula cuando lo que es reclamado es la resolución de la Agencia que establece una infracción y se impone una sanción.

El asesor del Comité Udi, señor Mery preguntó si en la letra h), cuando utiliza la expresión “que resuelve un procedimiento sancionatorio”, está dando a entender que solo sería reclamable aquella que impone una sanción.

El asesor del Ministerio de Hacienda, señor Godoy se mostró contrario a esa interpretación.

El Presidente de la Comisión, Honorable Senador señor Harboe sugirió reemplazar la frase final de la letra h), por la siguiente: “, dejar sin efecto o modificar la sanción impuesta o la absolución, según sea el caso.”.

Seguidamente decretó cerrado el debate del artículo 47.

En primer lugar sometió a votación las a), c), d), e), f), g), h) e i), del artículo 47.

La Comisión por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó el artículo 47 con las enmiendas señaladas precedentemente.

A continuación, **el señor Presidente de la Comisión**, **Honorable Senador señor Harboe,** sometió a votación la letra b) del artículo 47.

La Comisión, por mayoría de votos rechazó la letra b) del artículo 47. Se pronunciaron en contra los Honorables Senadores señores Araya y Harboe. Voto por su aprobación el Honorable Senador señor Larraín.

Artículo 48

Seguidamente, la Comisión analizó el artículo 48 del proyecto de ley del Ejecutivo, que encabeza un párrafo referido a la responsabilidad de los órganos públicos, de la autoridad o jefe superior del órgano y de sus funciones. Este artículo regula la responsabilidad administrativa de los jefes superiores de servicios en materia de tratamientos de datos. Su texto es el siguiente:

"Artículo 48.- Responsabilidad administrativa de la autoridad o jefe superior del órgano público. La autoridad o jefe superior de un órgano público debe velar para que el órgano respectivo realice el tratamiento de los datos personales con arreglo a los principios y obligaciones establecidos en el título IV de esta ley.

Las infracciones a los principios y obligaciones establecidos en esta ley por parte del órgano público serán sancionadas con multa de 20% a 50% de la remuneración mensual de la autoridad o jefe superior del órgano público infractor. La cuantía de la multa se determinará considerando la gravedad de la infracción, la naturaleza de los datos tratados y el número de titulares afectados.

Si el órgano público persiste en la infracción, se le aplicará a la autoridad o jefe superior del órgano público el duplo de la sanción originalmente impuesta y la suspensión en el cargo por un lapso de cinco días.

Tratándose de datos personales sensibles, la multa será del 50% de la remuneración mensual de la autoridad o jefe superior del órgano público y procederá la suspensión en el cargo de hasta treinta días.

Las infracciones en que incurra un órgano público en el tratamiento de los datos personales serán determinadas por la Agencia de Protección de Datos Personales, en virtud de una fiscalización de oficio o como resultado de un reclamo o denuncia presentada por un particular.

Las sanciones administrativas señaladas en este artículo serán aplicadas por la Contraloría General de la República, previa instrucción de una investigación sumaria, de acuerdo a las normas de su ley orgánica. El procedimiento administrativo correspondiente podrá ser iniciado directamente por la Contraloría General de la República o a requerimiento de la Agencia de Protección de Datos Personales. En la investigación administrativa la Contraloría General de la República deberá tomar en consideración el informe emanado de la Agencia de Protección de Datos Personales.

En la determinación de la responsabilidad administrativa de la autoridad o jefe superior del órgano público se deben considerar las circunstancias que atenúan su responsabilidad, especialmente la establecida en el inciso final del artículo 41.

Las sanciones previstas en este artículo deberán ser publicadas en el sitio web de la Agencia de Protección de Datos Personales y del respectivo órgano o servicio, conforme al artículo 7 de la ley de Transparencia de la Función Pública y de Acceso a la Información de la Administración del Estado, contenida en el artículo primero de la ley N° 20.285, dentro del plazo de cinco días hábiles, contados desde que la respectiva resolución quede firme.”.

Al iniciarse el estudio de este precepto, **los representantes del Ejecutivo, señora Piedrabuena y señor Godoy**, propusieron a la Comisión aprobar este precepto, enmendado en los siguientes términos:

“Artículo 48.- Responsabilidad administrativa de la autoridad o jefe superior del órgano público. La autoridad o jefe superior de un órgano público deberá velar para que el órgano respectivo realice sus operaciones y actividades de tratamiento de los datos personales con arreglo a los principios, derechos y obligaciones establecidos en el Título IV de esta ley.

Las infracciones a los principios, derechos y obligaciones en que puedan incurrir los órganos públicos se tipifican en los artículos 38 bis, 38 ter y 38 quáter y serán sancionadas con multa de 20% a 50% de la remuneración mensual de la autoridad o jefe superior del órgano público infractor. La cuantía de la multa se determinará considerando la gravedad de la infracción, la naturaleza de los datos tratados y el número de titulares afectados. En la determinación de la sanción se deberán considerar también las circunstancias que atenúan la responsabilidad del infractor, especialmente la establecida en el inciso final del artículo 41.

Si el órgano público persiste en la infracción, se le aplicará a la autoridad o jefe superior del órgano público el duplo de la sanción originalmente impuesta y la suspensión en el cargo por un lapso de cinco días.

Tratándose de datos personales sensibles, la multa será del 50% de la remuneración mensual de la autoridad o jefe superior del órgano público y procederá la suspensión en el cargo de hasta treinta días.

Las infracciones en que incurra un órgano público en el tratamiento de los datos personales serán determinadas por la Agencia de Protección de Datos Personales de acuerdo al procedimiento establecido en el artículo 46.

Habiéndose configurado la infracción, las sanciones administrativas señaladas en este artículo serán aplicadas por la Agencia de Protección de Datos Personales. Con todo, la Contraloría General de la República, de oficio o a petición de la Agencia de Protección de Datos Personales podrá, de acuerdo a las normas de su ley orgánica, incoar los procedimientos administrativos y establecer las sanciones que correspondan.

En contra de las resoluciones de la Agencia de Protección de Datos Personales se podrá deducir el reclamo de ilegalidad establecido en el artículo 47.

Las sanciones previstas en este artículo deberán ser publicadas en el sitio web de la Agencia de Protección de Datos Personales y del respectivo órgano o servicio, dentro del plazo de cinco días hábiles, contados desde que la respectiva resolución quede firme.”.

El señor Presidente de la Comisión sugirió a la Comisión pronunciarse separadamente respecto a cada inciso que contiene esta disposición.

En relación al inciso primero se sugirió suprimir la expresión “la autoridad o” las dos veces que aparece.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores De Urresti, Harboe, Larraín y Prokurica, aprobó el inciso primero del artículo 48, con la enmienda indicada.

A continuación, se puso en votación el inciso segundo de la nueva propuesta del Ejecutivo.

El asesor del Comité Udi, señor Mery, consideró abstracta la remisión a los principios, derechos y obligaciones. Agregó que toda referencia a los principios puede ser problemática en la interpretación. Sugirió que la remisión se realice a artículos determinados.

El asesor del Honorable Senador Larraín, señor Olmedo, constató que en lo que se refiere a este cuerpo legal, la autoridad es el jefe superior del servicio.

El Honorable Senador señor Larraín propuso eliminar el término “de la autoridad”.

El Presidente de la Comisión, Honorable Senador señor Harboe, sostuvo que si se adopta lo propuesto por el asesor, señor Mery, y el jefe de servicio vulnera el principio de reserva o el de la autodeterminación informativa, no habría sanción porque no está recogido en el catálogo de infracciones. Atendido lo anterior, se mostró partidario de conservar la redacción propuesta.

El asesor del Ministerio de Hacienda, señor Godoy, aseveró que el artículo 38 que inicia la tipificación de las infracciones, parte señalando: “Artículo 38.- Infracciones leves, graves y gravísimas. Las infracciones cometidas por los responsables de datos a los principios, derechos y obligaciones establecidos en esta ley se califican, atendida su gravedad, en leves, graves y gravísimas.”.

Dada la anterior redacción, insistió en mantener el tenor del inciso segundo del artículo 48.

El Presidente de la Comisión, Honorable Senador señor Harboe declaró cerrado el debate del inciso segundo.

La Comisión por la unanimidad de los Honorables Senadores presentes, señores De Urresti, Harboe, Larraín y Prokurica, aprobó el inciso segundo, con la enmienda de reemplazar la expresión “de la autoridad o” por “del”.

En relación al inciso tercero, **el señor Presidente de la Republica**, propuso aprobarlo sustituyendo la expresión “a la autoridad o” por “al”.

La Comisión por la unanimidad de sus miembros presentes, Honorables Senadores señores De Urresti, Harboe, Larraín y Prokurica, aprobó el inciso tercero, con la enmienda indicada.

En seguida, se puso en votación los incisos cuarto y quinto.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores De Urresti, Harboe, Larraín y Prokurica, aprobó ambos incisos del artículo 48.

A continuación, **el señor Presidente** puso en discusión el inciso sexto.

El Presidente de la Comisión, Honorable Senador señor Harboe, advirtió que en este inciso se contempla la posibilidad de que dos instituciones apliquen sanciones. Preguntó qué fundamenta esta regla.

El asesor del Ministerio de Hacienda, señor Godoy, aseveró que se unificaron los procedimientos infraccionales y de la autoridad que aplica la sanción, entre los responsables de datos privados y los órganos públicos.

Agregó que el modelo que se adoptó para el establecimiento de la responsabilidad de los órganos públicos, fue el del Consejo para la Transparencia.

El asesor del Comité Udi, señor Mery, manifestó sus dudas respecto a la frase: “y establecer las sanciones que correspondan.”. Afirmó que la potestad punitiva en esta materia está radicada en la Agencia de Protección de Datos Personales.

El Presidente de la Comisión, Honorable Senador señor Harboe sugirió la siguiente redacción a la segunda parte del inciso sexto:

“Con todo, la Contraloría General de la República, a petición de la Agencia de Protección de Datos Personales podrá, de acuerdo a las normas de su ley orgánica, incoar los procedimientos administrativos.”.

La redacción propuesta permite dejar radicado en la Agencia la posibilidad de solicitar a la Contraloría que lleve a cabo un procedimiento administrativo. Asimismo, la potestad sancionadora queda reservada a la mencionada Agencia.

El asesor del Ministerio de Hacienda, señor Godoy, aseveró que en la parte inicial de este inciso se señala que quien aplica la sanción es siempre la Agencia.

Atendido lo anterior, **el Presidente de la Comisión, Honorable Senador señor Harboe** sugirió un nuevo texto, a saber:

"Con todo, la Contraloría General de la República, a petición de la Agencia de Protección de Datos Personales podrá, de acuerdo a las normas de su ley orgánica, incoar los procedimientos administrativos y proponer las sanciones que correspondan."

Seguidamente, **el señor Presidente de la Comisión** declaró cerrado el debate y puso en votación el inciso sexto.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores De Urresti, Harboe, Larraín y Prokurica, aprobó el inciso sexto, en los términos indicados precedentemente.

En seguida, **el señor Presidente de la Comisión** puso en discusión el inciso séptimo enmendado en la nueva propuesta del Ejecutivo.

El asesor del Honorable Senador Larraín, **señor Olmedo,** hizo presente que el hecho de excluir cualquier otro recurso administrativo por parte de la Administración del Estado, implica que se debe concurrir a los tribunales de justicia. Lo anterior implica que el Servicio deberá asumir el costo de esos litigios en contra de la Agencia.

El asesor del Ministerio de Hacienda, señor Godoy, destacó que solo en el evento en que la representación judicial de la Agencia se deba asumir en regiones, será el Consejo de Defensa del Estado el encargado de hacerlo.

Concluido el debate, **el señor Presidente de la Comisión**, puso en votación el inciso séptimo.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores De Urresti, Harboe, Larraín y Prokurica, aprobó esta disposición.

Finalmente, **el señor Presidente de la Comisión** puso en discusión el inciso octavo**.**

El Honorable Senador señor Larraín preguntó si las sanciones son notificadas.

El Presidente de la Comisión, Honorable Senador señor Harboe, precisó que las sanciones son notificadas y que en

el inciso en estudio se contempla un requisito adicional, a saber, la obligatoriedad de publicarlas en el sitio web de la Agencia de Protección de Datos Personales y del respectivo órgano o servicio.

El señor Presidente de la Comisión declaró cerrado el debate y puso en votación este inciso del artículo 48.

La Comisión por la unanimidad de sus miembros presentes, Honorables Senadores señores De Urresti, Harboe, Larraín y Prokurica, aprobó esta disposición.

El texto acordado precedentemente fue ratificado mediante una indicación que presentó el Ejecutivo, la que se dio por aprobada con las votaciones señaladas precedentemente.

Artículo 49

A continuación la Comisión consideró el artículo 49 del proyecto de ley del Ejecutivo, disposición que regula la responsabilidad del funcionario infractor de las disposiciones de esta ley. Este precepto dispone lo siguiente:

“Artículo 49.- Responsabilidad del funcionario infractor. Sin perjuicio de lo dispuesto en el artículo anterior, si en el informe elaborado por la Agencia de Protección de Datos Personales o en el procedimiento de investigación sumaria o en el sumario administrativo que instruye la Contraloría General de la República, se determina que existen responsabilidades individuales de uno o más funcionarios del órgano público, la Contraloría General de la República iniciará una investigación sumaria para determinar las responsabilidades de dichos funcionarios o lo hará en el procedimiento administrativo ya iniciado. Las sanciones a los funcionarios infractores serán determinadas de conformidad a lo dispuesto en la ley N° 18.834.

En caso que el procedimiento administrativo correspondiente determine que cualquiera de los funcionarios involucrados es responsable de alguna de las infracciones graves o gravísimas señaladas en el artículo 38 de esta ley, esta conducta se considerará una falta grave a la probidad administrativa. En tales circunstancias, se podrá multar a estos funcionarios por hasta el doble del beneficio pecuniario obtenido mediante la infracción. En el evento de que no sea posible determinar el beneficio económico obtenido por los infractores, se podrá aplicar una multa de hasta el 50% de la remuneración mensual del funcionario.”.

Al iniciarse el estudio de esta materia, **los representantes del Ejecutivo, señora Piedrabuena y señor Godoy**,

sugirieron a la Comisión aprobar el proyecto de ley del Ejecutivo en los siguientes términos:

"Artículo 49.- Responsabilidad del funcionario infractor. Sin perjuicio de lo dispuesto en el artículo anterior, **si en el procedimiento administrativo** correspondiente se determina que existen responsabilidades individuales de uno o más funcionarios del órgano público, la Contraloría General de la República, **de oficio** o a petición de la Agencia de Protección de Datos Personales, iniciará una investigación sumaria para determinar las responsabilidades de dichos funcionarios o lo hará en el procedimiento administrativo ya iniciado, en su caso. Las sanciones a los funcionarios infractores serán determinadas de conformidad a lo dispuesto en el Estatuto Administrativo.

En caso que el procedimiento administrativo correspondiente determine que cualquiera de los funcionarios involucrados es responsable de alguna de las infracciones gravísimas señaladas en el artículo 38 quáter de esta ley, esta conducta se considerará una falta grave a la probidad administrativa. En tales circunstancias, se podrá multar a estos funcionarios por hasta el doble del beneficio pecuniario obtenido mediante la infracción. En el evento de que no sea posible determinar el beneficio económico obtenido por los infractores, se podrá aplicar una multa de hasta el 50% de la remuneración mensual del funcionario.".

Al comenzar el análisis de esta propuesta del Gobierno, **el señor Presidente de la Comisión**, **Honorable Senador señor Harboe**, sugirió a sus miembros considerar cada inciso de este artículo por separado.

En relación al inciso primero, **el señor Presidente de la Comisión** propuso eliminar la expresión "de oficio", para ser coherente con lo aprobado precedentemente.

La Comisión por la unanimidad de los Honorables Senadores presentes, señores De Urresti, Harboe, Larraín y Prokurica, aprobó el inciso primero, con la enmienda indicada precedentemente.

Respecto al inciso segundo, **el Honorable Senador señor Prokurica** consultó si la multa se aplica al sueldo líquido o bruto del funcionario.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena, afirmó que la multa recae sobre la remuneración mensual bruta.

El asesor del Comité Udi, señor Mery propuso, con la finalidad de guardar armonía con lo dispuesto por la Ley Orgánica Constitucional de Bases Generales de la Administración del Estado, se reemplace la expresión “falta grave” por “contravención grave”.

Seguidamente, el señor Presidente de la Comisión declaró cerrado el debate y puso en votación el inciso segundo, con la enmienda propuesta.

La Comisión por la unanimidad de los Honorables Senadores presentes, señores De Urresti, Harboe, Larraín y Prokurica, aprobó el inciso segundo, con la modificación señalada.

El texto acordado precedentemente fue ratificado mediante una indicación que presentó el Ejecutivo, la que se dio por aprobada con las votaciones señaladas precedentemente.

Artículo 50

Seguidamente, la Comisión analizó el artículo 50 del proyecto de ley del Ejecutivo, disposición que establece el deber de reserva y confidencialidad de los funcionarios públicos en materia de protección de datos. El texto del proyecto establece lo siguiente:

“Artículo 50.- Deberes de reserva y confidencialidad. Los funcionarios de los órganos públicos que traten datos personales, y especialmente cuando se refieran a datos personales sensibles o datos relativos a la comisión y sanción de infracciones penales, civiles, administrativas y disciplinarias, deben guardar secreto o confidencialidad respecto de la información que tomen conocimiento en el ejercicio de sus cargos y abstenerse de usar dicha información con una finalidad distinta de la que corresponda a las funciones legales del órgano público respectivo, o utilizarla en beneficio propio o de terceros. Para efectos de lo dispuesto en el inciso segundo del artículo 125 de la ley N° 18.834, se estimará que los hechos que configuran infracciones a esta disposición vulneran gravemente el principio de probidad administrativa, sin perjuicio de las demás sanciones y responsabilidades que procedan.”.

Al iniciarse el estudio de esta materia, **los representantes del Ejecutivo, señora Piedrabuena y señor Godoy** sugirieron a la Comisión aprobar este precepto en los siguientes términos:

“Artículo 50.- Deber de los funcionarios de reserva y confidencialidad. Los funcionarios de los órganos públicos que traten datos personales y especialmente, cuando se refieran a datos personales sensibles o datos relativos a la comisión y sanción de infracciones penales, civiles,

administrativas y disciplinarias, deben guardar secreto o confidencialidad respecto de la información que tomen conocimiento en el ejercicio de sus cargos y abstenerse de usar dicha información con una finalidad distinta de la que corresponda a las funciones legales del órgano público respectivo o, utilizarla en beneficio propio o de terceros. Para efectos de lo dispuesto en el inciso segundo del artículo 125 del Estatuto Administrativo, se estimará que los hechos que configuren infracciones a esta disposición vulneran gravemente el principio de probidad administrativa, sin perjuicio de las demás sanciones y responsabilidades que procedan.

Cuando en cumplimiento de una obligación legal un órgano público comunica o cede a otro órgano público datos protegidos por normas de secreto o confidencialidad, el organismo público receptor y sus funcionarios, deberán tratarlos manteniendo la misma obligación de secreto o confidencialidad.”.

El Presidente de la Comisión, Honorable Senador señor Harboe precisó que el objetivo que busca la norma en estudio consiste en que el funcionario público que tiene acceso a datos personales sensibles no utilice mal esa información.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores De Urresti, Harboe, Larraín y Prokurica aprobó el texto propuesto precedentemente.

El texto acordado precedentemente fue ratificado mediante una indicación que presentó el Ejecutivo, la que se dio por aprobada con la votación señalada precedentemente.

Artículo 51

A continuación, la Comisión analizó el artículo 51 del proyecto de ley del Ejecutivo, disposición que estable la responsabilidad civil del responsable de datos. Este precepto encabeza un nuevo párrafo quinto que regula el tema de la responsabilidad civil. El texto del proyecto de ley del Ejecutivo es el siguiente:

“Artículo 51.- Norma general. El responsable de datos deberá indemnizar el daño patrimonial y moral que cause al o los titulares, cuando en sus operaciones de tratamiento de datos infrinja los principios y obligaciones establecidos en esta ley y les cause daño, sin perjuicio de los demás derechos que concede esta ley al o los titulares de datos.

La acción indemnizatoria señalada en el inciso anterior podrá interponerse una vez ejecutoriada la resolución que resolvió favorablemente el reclamo interpuesto ante la Agencia de Protección de Datos Personales o la sentencia se encuentre firme y ejecutoriada, en caso de haber presentado un reclamo judicial, y se tramitará de conformidad a las normas generales del Código de Procedimiento Civil.”.

Al comenzar el estudio de esta disposición, los representantes del Ejecutivo sugirieron a la Comisión aprobar el proyecto de ley del Gobierno, con los cambios que se destacan en la redacción que se transcribe a continuación:

“Artículo 51.- Norma general. El responsable de datos deberá indemnizar el daño patrimonial y **extrapatrimonial** que cause al o los titulares, cuando en sus operaciones de tratamiento de datos infrinja los principios, derechos y obligaciones establecidos en esta ley y les cause perjuicio, sin perjuicio de los demás derechos que concede esta ley al o los titulares de datos.

La acción indemnizatoria señalada en el inciso anterior podrá interponerse una vez ejecutoriada la resolución que resolvió favorablemente el reclamo interpuesto ante la Agencia de Protección de Datos Personales o la sentencia se encuentre firme y ejecutoriada, en caso de haber presentado un reclamo judicial, y se tramitará de conformidad a las **normas del procedimiento sumario establecidas en el artículo 680 y siguientes** del Código de Procedimiento Civil.”.

Al comenzar el estudio de este precepto, el señor Presidente de la Comisión propuso considerar separadamente cada uno de sus incisos.

Seguidamente, planteó la conveniencia de reemplazar en el inciso primero la expresión “sin perjuicio de”, por: “Lo anterior no obsta al ejercicio de”.

El asesor del Comité Udi, señor Mery consultó, respecto a la frase que hace referencia al daño que se cause a los titulares, si no se admite hipótesis de daños por repercusión.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena manifestó que solo se refiere a los titulares de los datos personales.

El Presidente de la Comisión, Honorable Senador señor Harboe declaró cerrado el debate en torno al inciso primero y lo puso en votación.

La Comisión por la unanimidad de los Honorables Senadores presentes, señores De Urresti, Harboe, Larraín y Prokurica, aprobó el mencionado inciso, con la enmienda sugerida por el Presidente de la Comisión.

A continuación, la Comisión examinó el inciso segundo. Al comenzar su estudio se tuvo presente que respecto de este tema la Excma. Corte Suprema señaló lo siguiente en su oficio N° 63-2017, de 3 de mayo del 2017.

"En primer inciso de este artículo no parece ofrecer mayores dificultades. No así el inciso segundo, cuya norma presenta a lo menos dos situaciones posibles de observar. Por una parte, omite regular aquellos casos en que se produzcan hipótesis de responsabilidad civil sin responsabilidad administrativa, es decir, que las personas podrían acceder directamente a la vía judicial, sin necesidad del reclamo administrativo; y por otra, asumiendo la postura de la Corte frente a los procedimientos contenciosos administrativos especiales, la exigibilidad de la indemnización debiera seguir la regla contemplada por el literal i) del artículo 151 de la Ley de Municipalidades, que dispone que "Cuando se hubiere dado lugar al reclamo, el interesado podrá presentarse a los tribunales ordinarios de justicia para demandar, conforme a las reglas del juicio sumario, la indemnización de los perjuicios que procedieren y ante el Ministerio Público, la investigación criminal que correspondiere. En ambos casos, no podrá discutirse la ilegalidad ya declarada". De este modo se incentivaría el uso de esta acción, ahorrando los costos que implica un juicio ordinario, y evitando posibles dilaciones injustas para el titular.".

Sobre esta observación, **el asesor del Ministerio de Hacienda, señor Godoy,** expresó que la segunda parte de la observación del Máximo Tribunal fue asumida y se estableció que las reglas procedimentales para perseguir la acción indemnizatoria serán las del juicio sumario.

Respecto de la observación que sea una acción independiente, aseveró que se perseveró en la propuesta inicial, que consiste en que la responsabilidad civil sea consecuencia de una conducta infraccional del responsable de datos. Por lo tanto, previamente se acredite en sede administrativa que se incurrió en la infracción y posteriormente se persigan los perjuicios.

El asesor del Comité Udi, señor Mery, advirtió que la diferencia de opiniones es solo aparente, porque la redacción propuesta por la Excma. Corte Suprema no hace más que hacer referencia al sistema que opera en la Ley Orgánica Constitucional sobre Municipalidades que lo único que exige es que en la sentencia que acoge un reclamo de esta clase, se diga expresamente que en ese caso tiene derecho a reclamar los

perjuicios. Sugirió que traer la norma del estatuto municipal permitiría resolver el problema.

El Presidente de la Comisión, Honorable Senador señor Harboe preguntó si es necesario incorporar en la presente iniciativa la norma consagrada en la Ley Orgánica Constitucional sobre Municipalidades.

El asesor del Ministerio de Hacienda, señor Godoy respondió negativamente.

Seguidamente, el señor Presidente de la Comisión puso en votación el inciso segundo.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores De Urresti, Harboe, Larraín y Prokurica, aprobó esta disposición.

Seguidamente, la Comisión acordó incorporar a este precepto un inciso tercero que dispone lo siguiente:

“Las acciones civiles que deriven de una infracción a la presente ley prescribirán en el plazo de tres años, contados desde que se encuentre ejecutoriada la resolución administrativa o la sentencia judicial, según sea el caso, que imponga la multa respectiva.”.

Este acuerdo se adoptó por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Araya, De Urresti y Harboe.

Artículo 52

A continuación, la Comisión consideró el artículo 52 del proyecto de ley del Ejecutivo, disposición que regula los modelos de prevención de determinadas infracciones. Este precepto encabeza un párrafo sexto nuevo, referido precisamente a esta misma materia. El texto de este artículo es el siguiente:

“Artículo 52.- Modelo de prevención de infracciones. Los responsables de datos, sean personas naturales o entidades o personas jurídicas, públicas o privadas, podrán adoptar modelos de prevención de infracciones que deben contener, a lo menos, los siguientes elementos:

a) Designación de un encargado de prevención o delegado de protección de datos personales.

b) Definición de medios y facultades del encargado de prevención.

El responsable de datos debe disponer que el encargado de prevención cuente con los medios y facultades suficientes para el desempeño de sus funciones, debiendo otorgarle los recursos materiales necesarios para realizar adecuadamente sus labores, en consideración al tamaño y capacidad económica de la entidad.

c) Establecimiento de un programa de cumplimiento que deberá contemplar, a lo menos, lo siguiente:

i) La identificación del tipo de información que trata, el ámbito jurisdiccional en que opera, la categoría, clase o tipos de datos o bases de datos que administra, la caracterización de los titulares de datos y el o los lugares donde residen estos últimos.

ii) La identificación de las actividades o procesos de la entidad, sean habituales o esporádicos, en cuyo contexto se genere o incremente el riesgo de comisión de las infracciones señaladas en el artículo 38.

iii) El establecimiento de protocolos, reglas y procedimientos específicos que permitan a las personas que intervengan en las actividades o procesos indicados en la letra anterior, programar y ejecutar sus tareas o labores de una manera que prevenga la comisión de las referidas infracciones.

iv) Mecanismos de reporte hacia las autoridades para el caso de contravenir lo dispuesto en la presente ley.

v) La existencia de sanciones administrativas internas, así como de procedimientos de denuncia o persecución de responsabilidades de las personas que incumplan el sistema de prevención de infracciones.

d) Supervisión y certificación del modelo de prevención de infracciones.

La regulación interna a que dé lugar la implementación del modelo y el programa, en su caso, deberán ser incorporados expresamente como una obligación en los contratos de trabajo o de prestación de servicios de todos los trabajadores, empleados y prestadores de servicios de las entidades que actúen como responsables de datos o los terceros que efectúen el tratamiento, incluidos los máximos ejecutivos de la misma, o bien, como una obligación del reglamento interno

del que trata el artículo 153 y siguientes del Código del Trabajo. En este último caso, se deben realizar las medidas de publicidad establecidas en el artículo 156 del mismo Código.”.

Al iniciarse el estudio de esta disposición, **los representantes del Ejecutivo, señora Piedrabuena y señor Godoy**, sugirieron a la Comisión aprobar el proyecto del Gobierno enmendado en los siguientes términos.

Artículo 52.- Modelo de prevención de infracciones. Los responsables de datos, sean personas naturales o entidades o personas jurídicas, públicas o privadas, **podrán adoptar** modelos de prevención de infracciones que deben contener, a lo menos, los siguientes elementos:

a) Designación de un encargado de prevención o delegado de protección de datos personales.

b) Definición de medios y facultades del encargado de prevención.

El responsable de datos debe disponer que el encargado de prevención cuente con los medios y facultades suficientes para el desempeño de sus funciones, debiendo otorgarle los recursos materiales necesarios para realizar adecuadamente sus labores, en consideración al tamaño y capacidad económica de la entidad.

c) Establecimiento de un programa de cumplimiento que deberá contemplar, a lo menos, lo siguiente:

1. La identificación del tipo de información que la entidad trata, el ámbito territorial en que opera, la categoría, clase o tipos de datos o bases de datos que administra, la caracterización de los titulares de datos y el o los lugares donde residen estos últimos.

2. La identificación de las actividades o procesos de la entidad, sean habituales o esporádicos, en cuyo contexto se genere o incremente el riesgo de comisión de las infracciones señaladas en los artículos 38 bis, 38 ter y 38 quater.

3. El establecimiento de protocolos, reglas y procedimientos específicos que permitan a las personas que intervengan en las actividades o procesos indicados en la letra anterior, programar y ejecutar sus tareas o labores de una manera que prevenga la comisión de las referidas infracciones.

4. Mecanismos de reporte hacia las autoridades para el caso de contravenir lo dispuesto en la presente ley.

5. La existencia de sanciones administrativas internas, así como de procedimientos de denuncia o persecución de responsabilidades de las personas que incumplan el sistema de prevención de infracciones.

d) Supervisión y certificación del modelo de prevención de infracciones.

La regulación interna a que dé lugar la implementación del modelo y el programa, en su caso, deberán ser incorporadas expresamente como una obligación en los contratos de trabajo o de prestación de servicios de todos los trabajadores, empleados y prestadores de servicios de las entidades que actúen como responsables de datos o los terceros que efectúen el tratamiento, incluidos los máximos ejecutivos de la misma, o bien, como una obligación del reglamento interno del que trata el artículo 153 y siguientes del Código del Trabajo. En este último caso, se deben realizar las medidas de publicidad establecidas en el artículo 156 del mismo Código.”.

El Presidente de la Comisión, Honorable Senador señor Harboe expresó que la idea de incorporación del modelo de prevención es innovadora. Ella busca que el presente cuerpo legal no solo establezca obligaciones y le otorgue a la Agencia la capacidad para sancionar, sino que también incentive que la propia industria adecúe sus formas de trabajo con un modelo de prevención.

Agregó que la ventaja del mencionado modelo radica en que la industria contará con estándares más elevados de protección y además, actuará como un elemento a considerar ante una denuncia o infracción.

El Honorable Senador señor De Urresti indicó que la norma en estudio establece que será facultativo adoptar el modelo de prevención de infracciones. Propuso establecer el carácter imperativo del mismo. Por lo mismo, destacó que mantenerlo como facultativo le resta fuerza al modelo.

El Honorable Senador señor Larraín también hizo presente que le llama la atención que se establezca el modelo y que sea facultativo implementarlo. Reconoció que se puede imponer una fórmula intermedia que establezca una obligación mínima de prevención.

El Honorable Senador señor Prokurica se mostró partidario de lo señalado por los Honorables Senadores, señores De

Urresti y Larraín. Añadió que si se mantiene como facultativo, cuando se produce la infracción, debiera constituir una agravante para aquellas empresas que no han adoptado el modelo.

El Presidente de la Comisión, Honorable Senador señor Harboe, precisó que se debe perseguir que las empresas responsables de datos cuenten con mejores medidas para proteger los datos personales.

Reconoció que la técnica que acá se utiliza es similar a la empleada a propósito del Servicio Nacional del Consumidor. Expresó que para incentivar que los responsables de datos adopten dicho modelo, se consagra una atenuante en caso de que incurran en una infracción.

Puntualizó que si se establece la obligatoriedad de incorporar el modelo de prevención de infracciones, se debe agregar el incumplimiento del deber. Lo anterior puede llevar a sobrecargar a la Agencia en la fiscalización de la mencionada obligación.

Finalmente, enfatizó que en la legislación comparada, los modelos de prevención son voluntarios. Sin embargo, quienes no lo adoptan sufren mayores sanciones.

El Honorable Senador señor De Urresti insistió en que el modelo de prevención en Chile no ha funcionado adecuadamente. Por lo tanto, abogó que la implementación del mismo, sea obligatoria.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena afirmó que el hecho de establecer un modelo de prevención de infracciones de manera opcional responde a que la iniciativa en estudio está adoptando los estándares internacionales en materia de protección de datos.

Aseveró que también se siguió el modelo en la Comisión para el Mercado Financiero, a través de un modelo de autorregulación.

El Honorable Senador, señor De Urresti compartió lo expresado por la asesora, señora Piedrabuena. Sin embargo, se mostró partidario de elevar aún más el estándar.

Abogó que debe ser imperativa la implementación del modelo de prevención, al menos, para el sector público.

El Presidente de la Comisión Honorable Senador señor Harboe subrayó que el presente proyecto de ley viene a

cambiar completamente el estándar en materia de protección de datos personales.

Agregó que lo que viene a hacer el modelo de prevención es que por sobre dicho patrón, se pueda implementar el mencionado modelo, de manera de elevarlo aún más.

Se mostró de acuerdo con lo planteado por el Honorable Senador, señor De Urresti respecto a la obligatoriedad de que el modelo de prevención sea implementado a lo menos por el sector público.

Sugirió que aquellas instituciones privadas que quieran contratar con el Estado, deban contar con el mencionado modelo.

El asesor del Ministerio de Hacienda, señor Godoy, aclaró que la iniciativa viene a incrementar el estándar en materia de protección de datos. Aseveró que este último es uniforme para todos los responsables de datos, tanto del sector público como del privado.

Añadió que los modelos de cumplimiento vienen a facilitar la fiscalización por parte de la Agencia.

Asimismo, expresó que implementar el modelo de prevención tiene un costo. Agregó que para una persona natural resulta caro adoptarlo.

Hizo presente que para el sector público no representa una dificultad establecer los mencionados modelos. El incentivo para el cumplimiento en el sector público consiste en que la sanción se radica en el patrimonio del jefe de servicio.

El Honorable Senador señor Larraín manifestó que se puede establecer como obligatorio que exista un mecanismo de prevención, sin definirlo. Luego, consignó, que se puede agregar que podrán tener un modelo desarrollado, como el descrito en el presente artículo, en cuyo caso, si hubiese infracción se aplicará una atenuante.

El Honorable Senador señor De Urresti reconoció que constituye un gran incentivo el hecho de que la sanción recaiga en el patrimonio del jefe de servicio. Sin embargo, recordó que quien se ve afectado en caso de vulneración de esta ley es el ciudadano.

Insistió en que el modelo de prevención de infracciones debe ser obligatorio para el sector público.

El asesor del Honorable Senador Larraín, señor Olmedo, propuso a la Comisión que las empresas implementen una medida

de transparencia activa. Estimó que ella puede consistir en una publicación en la respectiva página web.

En sesión posterior, la Comisión continuó con el análisis del modelo de prevención de infracciones.

El asesor del Ministerio de Hacienda, **señor Godoy** propuso a la Comisión reemplazar el inciso primero de este artículo por los siguientes:

“Artículo 52.- Modelo de prevención de infracciones. Los responsables de datos, sean personas naturales o entidades o personas jurídicas, públicas o privadas, deberán adoptar mecanismos para prevenir la comisión de infracciones establecidas en los artículos 38 bis, 38 ter y 38 quáter.

Asimismo, los responsables de datos podrán voluntariamente adoptar modelos de prevención de infracciones, los que deberán contener a lo menos los siguientes elementos:”…

Al explicar esta proposición, señaló que ella busca, sin especificar medidas de prevención, que todos los responsables de datos, sean públicos o privados, deben adoptar medidas en ese sentido.

El Honorable Senador señor Larraín se mostró de acuerdo con la nueva redacción. Recalcó que se mantiene la obligatoriedad de fijar los mecanismos que garanticen un estándar. Agregó que la Agencia deberá incentivar que se implementen modelos más completos.

Sometido a votación el artículo 52, con la enmienda sugerida por el representante del Ejecutivo, fue aprobado por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Araya, Harboe y Larraín.

Artículo 53

A continuación, la Comisión trató el artículo 53 del proyecto de ley del Ejecutivo, disposición que regula la certificación, registro, supervisión del modelo de infracciones. El texto de este precepto es el siguiente:

“Artículo 53.- Certificación, registro, supervisión del modelo de prevención de infracciones y reglamento. La Agencia de Protección de Datos Personales será la entidad encargada de certificar que el modelo de prevención de infracciones y el programa de cumplimiento

reúna los requisitos y elementos establecidos en la ley y su reglamento, y supervisarlos.

La Agencia de Protección de Datos Personales creará un registro público en que consten las entidades que posean una certificación y aquellas cuya certificación sea revocada.

Un reglamento dictado por el Ministerio de Hacienda y suscrito por el Ministro o Ministra Secretario General de la Presidencia y por el Ministro o Ministra de Economía, Fomento y Turismo, establecerá los requisitos, modalidades y procedimientos para la implementación, certificación, registro y supervisión de los modelos de prevención de infracciones y los programas de cumplimiento.”.

Al iniciarse el estudio de este precepto, **el asesor del Ministerio de Hacienda, señor Godoy,** sostuvo que se propone que los modelos de prevención sean certificados por la Agencia de Protección de Datos. Agregó que en el derecho comparado son las empresas auditoras privadas las que certifican los modelos de prevención. Sin embargo, la experiencia a nivel nacional apunta que ello debe ser realizado por el órgano que se crea.

El Honorable Senador señor Larraín consultó si es conveniente que se faculte a la Agencia a delegar esta función en alguna entidad.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena manifestó que parece razonable que la Agencia pueda delegar. Sin embargo, expresó que se debe fijar en la ley los requisitos que deben cumplir las entidades que cumplirán ese rol.

El Honorable Senador señor De Urresti compartió la opinión de la asesora, señora Piedrabuena. Añadió que la experiencia de la acreditación universitaria fue nefasta para el sistema y para las propias instituciones.

Constató que se debe analizar la capacidad de la Agencia. Precisó que estamos ante un órgano centralizado, lo que dificulta el acceso a la certificación. Dado lo anterior, preguntó por la capacidad operativa de la autoridad mencionada.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena aseguró que la Agencia podrá subcontratar a una empresa que realice la labor de acreditación. Sin embargo, la responsabilidad final, recae en el órgano que se crea.

El Honorable Senador señor Larraín insistió en que nada obsta a que se autorice a la Agencia a contratar servicios que faciliten el cumplimiento del objetivo de acreditación.

Sugirió reemplazar en el inciso segundo la expresión: “sea revocada”, por “haya sido revocada”.

Al tenor de este debate, el Ejecutivo presentó una indicación para regular esta materia. El texto del artículo 53 es el siguiente:

“Artículo 53.- Certificación, registro, supervisión del modelo de prevención de infracciones y reglamento. La Agencia de Protección de Datos Personales será la entidad encargada de certificar que el modelo de prevención de infracciones y el programa de cumplimiento reúna los requisitos y elementos establecidos en la ley y su reglamento y supervisarlos.

La Agencia de Protección de Datos Personales creará un registro público en que consten las entidades que posean una certificación y aquellas cuya certificación haya sido revocada.

Un reglamento expedido por el Ministerio de Hacienda y suscrito por el Ministro Secretario General de la Presidencia y por el Ministro de Economía, Fomento y Turismo establecerá los requisitos, modalidades y procedimientos para la implementación, certificación, registro y supervisión de los modelos de prevención de infracciones y los programas de cumplimiento.”

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, De Urresti, Harboe y Larraín, aprobó esta redacción para el artículo 53.

Artículo 54

Seguidamente, la Comisión estudió el artículo 54 del proyecto de ley del Ejecutivo que establece una atenuante especial por prevención de infracciones. El texto de esta disposición es el siguiente:

“Artículo 54.- Atenuante especial por prevención de infracciones. Los responsables de datos que incurran en alguna de las infracciones previstas en el artículo 38 podrán atenuar su responsabilidad si acreditan haber cumplido diligentemente sus deberes de dirección y supervisión para la protección de los datos personales bajo su responsabilidad o tratamiento.

Se considera que los deberes de dirección y supervisión se han cumplido cuando, con anterioridad a la comisión de la infracción, los responsables de datos hubieren adoptado e implementado un modelo de organización, administración y supervisión para prevenir infracciones, lo que deberá constar en un certificado emitido por la Agencia de Protección de Datos Personales.”.

Al iniciarse el estudio de este precepto, **los representantes del Ejecutivo, señora Piedrabuena y señor Godoy**, propusieron a la Comisión aprobar este artículo, enmendado en los siguientes términos:

“Artículo 54.- Atenuante especial por prevención de infracciones. Los responsables de datos que incurran en alguna de las infracciones previstas en **los artículos 38 bis, 38 ter y 38 quáter**, podrán atenuar su responsabilidad si acreditan haber cumplido sus deberes de dirección y supervisión para la protección de los datos personales bajo su responsabilidad o tratamiento.

Se considera que los deberes de dirección y supervisión se han cumplido cuando, con anterioridad a la comisión de la infracción, los responsables de datos hubieren adoptado e implementado un modelo de organización, administración y supervisión para prevenir infracciones, lo que deberá constar en un certificado emitido por la Agencia de Protección de Datos Personales.”

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena expresó que si los responsables de datos quieren acceder a la atenuante especial deben tener implementado el modelo de prevención y contar con el certificado expedido por la Agencia.

El Honorable Senador señor Larraín sugirió que en la parte final del inciso primero, con posterioridad a la frase “haber cumplido”, se agregue la expresión “fielmente” o “adecuadamente”.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena precisó que la atenuante se configura al contar con el certificado antes mencionado. Remarcó que este último se otorga cuando el responsable ha implementado el modelo de administración y supervisión para prevenir infracciones.

El Honorable Senador señor De Urresti preguntó por el plazo de vigencia de la certificación.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena destacó que en el artículo siguiente se responde lo consultado. Agregó que en él se contemplan las causales de revocación.

El Honorable Senador señor De Urresti consideró relevante construir un buen instrumento que permita elevar el estándar.

El asesor del Ministerio de Hacienda, señor Godoy, afirmó que con la propuesta se avanzó a un modelo de responsabilidad lo más objetivo posible. Añadió que los modelos de prevención constituyen una presunción. Subrayó que cuando un responsable de datos presenta un modelo que cumpla las exigencias mínimas establecidas en la ley, surge la presunción de que éste tiene un nivel adecuado de cumplimiento de las obligaciones establecidas en la ley.

Sostuvo que los modelos de prevención constituyen una ayuda a la fiscalización.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena manifestó que la ISO 27001 es una norma que dice relación con la seguridad de la información. En ella se establece que los modelos certificados tienen una duración de tres años. Por lo tanto, dicho plazo es concordante con el término consagrado en la presente iniciativa.

En esta parte del debate, los representantes del Ejecutivo propusieron agregar, luego de la palabra “cumplido”, las dos veces que aparece, la expresión “fehacientemente”.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó esta disposición con las enmiendas indicadas.

Artículo 55

Seguidamente, la Comisión examinó el artículo 55 del proyecto de ley del Ejecutivo. Este precepto regula la vigencia de los certificados expedidos por la Agencia de Protección de Datos Personales. Su texto es el siguiente:

“Artículo 55.- Vigencia de los certificados. Los certificados expedidos por la Agencia de Protección de Datos Personales tendrán una vigencia de tres años. Sin perjuicio de lo anterior, quedarán sin efecto en los siguientes casos:

a) Por revocación efectuada por la Agencia de Protección de Datos Personales.

b) Por fallecimiento del responsable de datos en caso de tratarse de una persona natural o por disolución de la persona jurídica.

c) Por resolución judicial ejecutoriada.

d) Por cese voluntario de la actividad del responsable de datos.

El término de vigencia de un certificado por alguna de las causales señaladas precedentemente será inoponible a terceros mientras no sea eliminado del registro.”

Al iniciarse el estudio de este precepto, **el Honorable Senador, señor De Urresti**, preguntó, en referencia a la letra b), en qué casos la persona natural es responsable de datos.

El asesor del Ministerio de Hacienda, señor Godoy, precisó que una persona natural puede administrar datos en el ejercicio de sus actividades profesionales o comerciales. Ejemplificó con el caso de un médico, quien administra datos de sus pacientes.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena destacó que el artículo 1° se define el ámbito de aplicación de la ley, y ella incluye a las personas naturales que realicen tratamiento de datos.

El Honorable Senador señor Larraín recomendó separar en letras distintas, las dos causales consagradas en la letra b).

El Ejecutivo, para acoger esta propuesta, presentó una indicación sustitutiva de este precepto que establece lo siguiente:

“Artículo 55.- Vigencia de los certificados. Los certificados expedidos por la Agencia de Protección de Datos Personales tendrán una vigencia de tres años. Sin perjuicio de lo anterior, quedarán sin efecto en los siguientes casos:

a) Por revocación efectuada por la Agencia de Protección de Datos Personales.

b) Por fallecimiento del responsable de datos en los casos de personas naturales.

c) Por disolución de la persona jurídica.

d) Por resolución judicial ejecutoriada.

e) Por cese voluntario de la actividad del responsable de datos.

El término de vigencia de un certificado por alguna de las causales señaladas precedentemente será inoponible a terceros, mientras no sea eliminado del registro.”.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó esta disposición.

Artículo 56

En seguida, la Comisión trató el artículo 56 del proyecto de ley del Ejecutivo, disposición que regula la revocación de las certificaciones que emite la Agencia de Protección de datos. Su texto es el siguiente:

“Artículo 56.- Revocación de la certificación. La Agencia de Protección de Datos Personales puede revocar la certificación indicada en los artículos precedentes si el responsable no da cumplimiento a lo establecido en este párrafo. Con este objeto la Agencia de Protección de Datos Personales podrá requerir toda aquella información que fuere necesaria para el ejercicio de sus funciones.

Los responsables pueden exceptuarse de entregar la información solicitada cuando ésta esté amparada por una obligación de secreto o confidencialidad, debiendo acreditar dicha circunstancia.

El incumplimiento en la entrega de la información requerida, así como la entrega de información falsa, incompleta o manifiestamente errónea será sancionado en conformidad con esta ley.

Cuando un certificado haya sido revocado por la Agencia de Protección de Datos Personales para volver a solicitarlo el responsable de datos debe acreditar fehacientemente que la causal que dio origen a su revocación ha sido subsanada.”

Al iniciarse el estudio de este precepto, **el asesor del Ministerio de Hacienda, señor Godoy,** recordó que la letra k), del artículo 38 quater, consagra, dentro de las infracciones gravísimas, la siguiente:

“k) Entregar información falsa, incompleta o manifiestamente errónea en el proceso de registro o certificación del modelo de prevención de infracciones.”.

Agregó que si a algún responsable se le revoca el certificado, podrá volver a solicitarlo, siempre que pruebe haber subsanado la causal de cancelación.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó esta disposición.

Artículo 57

Seguidamente, trató el artículo 57 del proyecto de ley del Ejecutivo, disposición que encabeza un título referido al tratamiento de datos personales en el Congreso Nacional, el Poder Judicial y en organismos dotados de autonomía constitucional, y cuyo objeto es regular el tratamiento de datos personales por las instituciones mencionadas. El texto de esta disposición es la siguiente:

“Artículo 57.- Regla general del tratamiento de datos personales. Es lícito el tratamiento de los datos personales que efectúan el Congreso Nacional, el Poder Judicial, la Contraloría General de la República, el Ministerio Público, el Tribunal Constitucional, el Banco Central, el Servicio Electoral y la Justicia Electoral, y los demás tribunales especiales creados por ley, cuando se realiza para el cumplimiento de sus funciones legales, dentro del ámbito de sus competencias y de conformidad a las normas especiales que se establecen en sus respectivas leyes orgánicas y a las disposiciones del título IV de esta ley aplicables a los órganos públicos, con excepción de lo dispuesto en el artículo 14 quinquies. En esas condiciones, estas instituciones y organismos detentan la calidad de responsables de datos y no requieren el consentimiento del titular para efectuar el tratamiento de sus datos personales.

Corresponde a los órganos internos de las instituciones y organismos señalados en el inciso anterior ejercer las funciones y adoptar las decisiones que esta ley encomienda a la Agencia de Protección de Datos Personales.

Las autoridades superiores de los órganos internos de estas instituciones deberán dictar las políticas, normas e instrucciones necesarias para dar cumplimiento a los principios y obligaciones establecidos en esta ley, especialmente aquéllas que permitan el ejercicio de los derechos que se reconocen a los titulares de datos y las que fijan los estándares o condiciones mínimas de control, seguridad y

resguardo que se deben observar en el tratamiento de los datos personales, pudiendo requerir para ello la asistencia técnica de la Agencia de Protección de Datos Personales. Asimismo, las autoridades de estos órganos ejercerán la potestad disciplinaria respecto de sus funcionarios, en relación a las infracciones que se produzcan en el tratamiento de los datos personales.

Las instituciones y órganos señalados en este artículo no estarán sujetos a la regulación, fiscalización o supervigilancia de la Agencia de Protección de Datos Personales.”.

Al iniciarse el debate de este precepto, **los representantes del Ejecutivo, señora Piedrabuena y señor Godoy**, propusieron a la Comisión aprobar el texto del Ejecutivo, con una enmienda que consiste en agregar en el inciso tercero de esta disposición una frase que precise que las infracciones que interesa sancionar son las señaladas en los artículos 38 bis, 38 ter y 38 quater de la ley.

Agregó el **asesor del Ministerio de Hacienda, señor Godoy,** que el título VIII tiene como fundamento el tratar de regular el tratamiento de datos personales en los organismos con autonomía constitucional. Puntualizó que algunos de ellos son parte de la Administración del Estado pero se rigen por un estatuto jurídico particular. Desde esa perspectiva, no se pueden sujetar a la fiscalización o a la tutela de la Agencia.

Hizo presente que la ley es obligatoria, desde el punto de vista de los derechos y deberes para las mencionadas instituciones. Añadió que los regímenes sancionatorios y específicos de cumplimiento al interior de la respectiva institución queda entregado a las máximas autoridades de estos organismos autónomos.

El Honorable Senador señor Larraín reflexionó acerca de la conveniencia de fijar en esta norma el organismo que deba realizar el control y la supervisión.

El Honorable Senador señor De Urresti preguntó por qué no se considera en este artículo a las Fuerzas Armadas y a Televisión Nacional de Chile.

El asesor del Ministerio de Hacienda, señor Godoy afirmó que las Fuerzas Armadas forman parte de los órganos de la Administración del Estado. Por lo tanto, están sujetas al Título IV de este cuerpo legal, salvo en lo que dice relación con las labores de la defensa de la Nación.

Agregó que respecto a las empresas públicas, ellas son responsables de datos como cualquier otro ente de la misma

naturaleza. Constató que Televisión Nacional de Chile carece de un estatuto específico.

Seguidamente**,** sugirió agregar en el inciso primero, luego de la expresión “14 quinquies”, la siguiente frase: “y de lo dispuesto en el artículo 50 en lo referente a la aplicación del Estatuto Administrativo.”.

Aclaró que se persigue que los funcionarios de los órganos con autonomía constitucional queden sujetos al deber de reserva y confidencialidad que consagra el artículo 50 del cuerpo legal en estudio, y que no queden regulados por las reglas del estatuto administrativo, para efectos de establecer su responsabilidad administrativa.

Con el fin de precisar de mejor manera esta materia, el Ejecutivo hizo llegar una indicación en la que se establece lo siguiente:

“Artículo 57.- Regla general del tratamiento de datos personales. Es lícito el tratamiento de los datos personales que efectúan el Congreso Nacional, el Poder Judicial, la Contraloría General de la República, el Ministerio Público, el Tribunal Constitucional, el Banco Central, el Servicio Electoral y la Justicia Electoral, y los demás tribunales especiales creados por ley, cuando se realiza para el cumplimiento de sus funciones legales, dentro del ámbito de sus competencias y, de conformidad a las normas especiales que se establecen en sus respectivas leyes orgánicas y a las disposiciones del título IV de esta ley aplicables a los órganos públicos, con excepción de lo dispuesto en el artículo 14 quinquies **y de lo dispuesto en el artículo 50 en lo referente a la aplicación del Estatuto Administrativo**. Los funcionarios de estos organismos deberán guardar reserva de tales datos. En esas condiciones estas instituciones y organismos detentan la calidad de responsables de datos y no requieren el consentimiento del titular para efectuar el tratamiento de sus datos personales.

Corresponde a los órganos internos de las instituciones y organismos señalados en el inciso anterior ejercer las funciones y adoptar las decisiones que esta ley encomienda a la Agencia de Protección de Datos Personales.

Las autoridades superiores de los órganos internos de estas instituciones deberán dictar las políticas, normas e instrucciones necesarias para dar cumplimiento a los principios y obligaciones establecidos en esta ley, especialmente aquellas que permitan el ejercicio de los derechos que se reconocen a los titulares de datos y las que fijan los estándares o condiciones mínimas de control, seguridad y resguardo que se deben observar en el tratamiento de los datos personales,

pudiendo requerir para ello la asistencia técnica de la Agencia de Protección de Datos Personales. Asimismo, las autoridades de estos órganos ejercerán la potestad disciplinaria respecto de sus funcionarios, en relación a las infracciones que se produzcan en el tratamiento de los datos personales, particularmente las infracciones señaladas en los artículos 38 bis, 38 ter y 38 quater.

Las instituciones y organismos señalados en este artículo no estarán sujetas a la regulación, fiscalización o supervigilancia de la Agencia de Protección de Datos Personales.”.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, De Urresti, Harboe y Larraín, aprobó este precepto en los términos propuestos en la indicación del Ejecutivo.

Artículo 58

A continuación, la Comisión examinó el artículo 58 del proyecto de ley del Ejecutivo que establece y regula los mecanismos para que los particulares puedan ejercer sus derechos ante los organismos autónomos señalados en el artículo precedente. El texto propuesto por el Mensaje es el siguiente:

“Artículo 58.- Ejercicio de los derechos y reclamaciones. Los titulares de datos ejercerán los derechos que le reconoce esta ley ante el Congreso Nacional, el Poder Judicial, la Contraloría General de la República, el Ministerio Público, el Tribunal Constitucional, el Banco Central, el Servicio Electoral y la Justicia Electoral, y los demás tribunales especiales creados por ley, de acuerdo a los procedimientos que dispongan estas instituciones y organismos para estos efectos, de conformidad a lo señalado en el artículo anterior.

En caso que el Congreso Nacional, la Contraloría General de la República, el Ministerio Público, el Banco Central o el Servicio Electoral denieguen injustificada o arbitrariamente el ejercicio de un derecho reconocido por esta ley a un titular de datos, o bien infrinjan algún principio, deber u obligación establecida en ella, causándole perjuicio, el titular que se vea agraviado o afectado por la decisión del organismo, podrá reclamar ante la Corte de Apelaciones, de acuerdo al procedimiento dispuesto en el artículo 47 de esta ley.

Las autoridades superiores del Poder Judicial, del Tribunal Constitucional, de la Justicia Electoral y de los demás tribunales especiales creados por ley, deberán asegurarse que en el tratamiento de los datos personales que realizan estas instituciones se cumplen estrictamente

con los principios y deberes, y se respeten los derechos de los titulares establecidos en esta ley, adoptando las medidas de fiscalización y control interno que resulten necesarias y adecuadas para esta finalidad.”.

Al iniciarse el estudio de este precepto, **el Honorable Senador señor Larraín** sugirió reemplazar la última frase del inciso primero que señala: “de acuerdo a los procedimientos que dispongan estas instituciones y organismos para estos efectos, de conformidad a lo señalado en el artículo anterior.”, por la siguiente: “de acuerdo a los procedimientos y ante los organismos que dispongan estas instituciones para estos efectos.”.

No se mostró partidario que en caso que los organismos descritos en el inciso segundo denieguen injustificada o arbitrariamente el ejercicio de un derecho reconocido por esta ley a un titular de datos, o bien infrinjan algún principio, deber u obligación establecida en ella, causándole perjuicio, el titular que se vea agraviado o afectado por la decisión del organismo, pueda reclamar ante la Corte de Apelaciones.

Enfatizó que cada institución debe contar con un mecanismo interno de resolución de ese tipo de conflictos. Ello preserva de mejor manera la autonomía de los poderes públicos.

El asesor del Ministerio de Hacienda, señor Godoy, manifestó que la mayor complejidad que tienen nuestros organismos autónomos es que en nuestra legislación no existe un estatuto que regule sus decisiones. Subrayó que en el balance de las autonomías de estos organismos, versus la tutela del ejercicio de los derechos de las personas, se estimó deseable avanzar en consagrar un sistema de tutela y de revisión por la vía judicial.

Consideró razonable que respecto al Congreso Nacional se establezca un modelo similar al del Poder Judicial. Reflexionó si aquello se puede replicar en los otros órganos que cuentan con autonomía constitucional, pero que no son poderes del Estado. En este último caso podría consagrarse la revisión judicial de sus decisiones.

El Honorable Senador señor Larraín recalcó que es partidario de salvaguardar la autonomía de los organismos mencionados y no judicializaría sus decisiones.

Indicó que cada institución deberá fijar un procedimiento que garantice una revisión adecuada para el caso específico.

En esta parte del debate, se recordó el artículo 4° de la Ley Orgánica Constitucional del Congreso Nacional, consagra un

procedimiento interno para casos relacionados con el acceso del público a la información.

La mencionada disposición prescribe lo siguiente en sus incisos segundo, tercero y cuarto:

“Las Cámaras establecerán en sus reglamentos las disposiciones que cautelen el acceso del público a la información, de conformidad al artículo sexto de la ley N° 20.285.

Los referidos reglamentos deberán señalar las autoridades u organismos internos encargados de responder las consultas que se formulen y el procedimiento a que se sujetarán los reclamos. Sin perjuicio de las causales establecidas en esta ley, se podrá denegar la entrega de información en virtud de las señaladas en los artículos 21 y 22 de Ley de Transparencia de la Función Pública y Acceso a la Información de la Administración del Estado, contenida en el artículo primero de la ley N° 20.285.

Las reclamaciones se resolverán en única instancia por la Comisión de Ética y Transparencia del Senado o de la Cámara de Diputados, según corresponda. Lo dispuesto en los artículos 24 a 30 y 33 de la Ley de Transparencia de la Función Pública y de Acceso a la Información de la Administración del Estado no se aplicará al Congreso Nacional ni a sus servicios comunes.”.

El asesor del Ministerio de Hacienda, señor Godoy, hizo presente que respecto de la Administración del Estado se generan situaciones asimétricas entre los demás poderes del Estado. Agregó que los mecanismos de control del Congreso Nacional son distintos de los demás órganos que cuentan con autonomía constitucional que han ido surgiendo.

Seguidamente, propuso a la Comisión introducir los siguientes cambios a este precepto:

En el inciso primero, reemplazar la expresión “de acuerdo a los procedimientos que dispongan estas instituciones y organismos para estos efectos,” por “de acuerdo a los procedimientos y ante los organismos que dispongan estas instituciones,”.

En el inciso segundo, eliminar la expresión “el Congreso Nacional,”.

En el tercer inciso, insertar después de la expresión “superiores” la siguiente expresión: “de Senado y de la Cámara de Diputados,”.

El Presidente de la Comisión, Honorable Senador señor Harboe, propuso examinar separadamente cada una de las enmiendas sugeridas por los representantes del Ejecutivo.

En relación a la primera enmienda, **el Honorable Senador señor Araya** consultó si cuando se habla de las autoridades superiores del Poder Judicial y del Tribunal Constitucional, se refiere al Presidente de esas instituciones o al Pleno.

Sugirió se personalice en la figura de los respectivos presidentes. Agregó que puede interpretarse que por autoridades superiores se entendiera cada Presidente de cada Corte. Lo mismo en el caso del Tribunal Electoral.

El Presidente de la Comisión, Honorable Senador señor Harboe ratificó que cuando la ley consagra la autoridad superior, se entiende que en el caso del Poder Judicial se refiere al Presidente del Máximo Tribunal. Lo mismo respecto al Tribunal Calificador de Elecciones.

El asesor del Ministerio de Hacienda, señor Godoy aseveró que dependerá de la ley orgánica del respectivo órgano. Destacó que en el caso del Poder Judicial, este tipo de instrucciones se vierten en un auto acordado dictado por el Pleno de la Exma. Corte Suprema.

El Presidente de la Comisión, Honorable Senador señor Harboe sostuvo que considerando que son órganos autónomos, se les debe exigir que en los procedimientos que sigan en estas materias consagren las reglas para un justo y racional procedimiento. Enfatizó que su preocupación radica en cómo garantizar que el ciudadano pueda ejercer su derecho de protección de datos personales ante los órganos mencionados.

El Honorable Senador señor Larraín se mostró partidario de conservar la redacción y acoger las enmiendas propuestas por el Ejecutivo.

El Presidente de la Comisión, Honorable Senador señor Harboe reiteró que debe añadirse, a continuación de: “y ante los organismos que dispongan estas instituciones”, la frase: “deberán respetar el justo y racional procedimiento.”. Advirtió que con ello se establece un estándar legal a las instituciones, para que adopten procedimientos adecuados.

La Comisión, por unanimidad de sus presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó, con las enmiendas indicadas, el inciso primero del artículo 58.

En seguida, se examinó la propuesta de eliminar en el inciso segundo, la expresión “el Congreso Nacional,”.

La Comisión, por unanimidad de sus miembros presentes, los Honorables Senadores señores Araya, Harboe y Larraín, aprobó, el inciso segundo, con el cambio sugerido precedentemente.

En relación a la enmienda al inciso tercero que consiste en intercalar, después de la expresión “superiores”, la frase “de Senado y de la Cámara de Diputados,” **el Honorable Senador señor Larraín** sugirió que la norma solo haga referencia a las autoridades superiores del Congreso Nacional, sin hacer una distinción entre el Senado y la Cámara de Diputados.

La Comisión, por unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, concordó con el planteamiento del Honorable Senador Larraín.

Como consecuencia de los acuerdos alcanzados precedentemente, se dio por aprobado el artículo 58, con las enmiendas ya indicadas,

Artículo 59

A continuación, la Comisión trató el artículo 59 del proyecto de ley del Ejecutivo, disposición que se refiere a los reglamentos de ejecución de la ley. Su texto es el siguiente:

“Artículo 59.- Reglamentos. Sin perjuicio de los reglamentos específicos que se señalan en el texto de esta ley, a través de uno o más reglamentos del Ministerio de Hacienda y suscritos por el Ministro o Ministra Secretario General de la Presidencia, se establecerán las demás normas necesarias para la ejecución de la presente ley.”.

El asesor del Ministerio de Hacienda, señor Godoy, sugirió a la Comisión eliminar el artículo 59, ya que en el cuerpo legal en estudio se establecen diversos reglamentos específicos de ejecución. Por lo tanto, sería innecesaria la presente disposición.

La Comisión, por la unanimidad de los Honorables Senadores presentes, señores Araya, Harboe y Larraín aprobó la eliminación del artículo 59.

A continuación, el señor Presidente de la Comisión propuso examinar un artículo 43 contenido en el texto de la Moción que se refunde en este proyecto de ley, disposición que modifica la letra d) del artículo 33 del artículo primero de la ley N° 20.285 sobre Acceso a la Información Pública.

Cabe recordar que el artículo 33 de la mencionada ley regula las funciones del Consejo para la Transparencia. La letra d) de este artículo prescribe que corresponde a este organismo dictar instrucciones generales para el cumplimiento de la legislación sobre transparencia y acceso a la información por parte de los órganos del Estado, y requerir a éstos para que ajusten sus procedimientos y sistemas de atención de público a dicha legislación.

El artículo de la moción propone intercalar luego de la frase "legislación sobre transparencia y acceso a la información," la siguiente frase "y sobre protección de datos personales,".

Al iniciarse el estudio de esta disposición, se recordó que es atribución exclusiva del Ejecutivo fijar las funciones y atribuciones de los órganos públicos. Además se hizo presente que las normas sobre protección de datos personales son fijadas en esta nueva ley y serán desarrolladas en los reglamentos que regulen a la Agencia de Protección de Datos Personales.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, rechazó la modificación indicada.

Artículo 2°

Seguidamente, la Comisión examinó el artículo 2° contenido en el proyecto de ley del Ejecutivo, disposición que propone reemplazar letra m) del artículo 33 contenido en el artículo primero de la ley N° 20.285, sobre acceso a la información pública. La nueva norma establecería lo siguiente

“m) Velar por la protección de los datos de carácter personal con sujeción a lo dispuesto en la ley N° 19.628, en los ámbitos de la transparencia de la función pública y el acceso a la información.”.

Al iniciarse el debate sobre este artículo se recordó que la protección de los datos personales corresponderá a la Agencia de Protección de Datos.

En virtud de lo anterior, **los representantes del Ejecutivo, señora Piedrabuena y señor Godoy,** sugirieron a la Comisión rechazar esta disposición y en concordancia con lo propuesto por Gobierno en este proyecto de ley, suprimir la letra m) del artículo 33.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, acogió este planteamiento, por lo que aprobó esta propuesta.

Con la misma votación se acordó rechazar el artículo 44 contenido en la moción que se refunde en este informe y que proponía derogar la ley N° 19.628, sobre protección de la vida privada

Artículos Transitorios

A continuación, la Comisión trató los artículos transitorios contenidos en el proyecto de ley del Ejecutivo.

Artículo primero

Este precepto establece que las modificaciones a las leyes N° 19.628, sobre protección de la vida privada, y Nº 20.285, sobre acceso a la información pública, contenidas en el artículo primero y segundo, respectivamente, de la presente ley, entrarán en vigencia el día primero del mes décimo tercero posterior a la publicación de la presente ley en el Diario Oficial.

El asesor del Ministerio de Hacienda, señor Godoy, explicó que en la práctica el Ejecutivo propone un plazo de un año de vacancia de la ley.

El Presidente de la Comisión, Honorable Senador señor Harboe preguntó por qué se establecía un término tan prolongado para la entrada en vigencia de estas modificaciones legales.

El asesor del Ministerio de Hacienda, señor Godoy, consignó que durante dicho período debe implementarse la Agencia de Protección de Datos Personales y dictarse las normas reglamentarias de ejecución.

El Presidente de la Comisión, Honorable Senador señor Harboe declaró cerrado el debate y sometió a votación el artículo primero transitorio.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó sin enmiendas este artículo.

Artículo segundo

Este artículo del proyecto del Ejecutivo prescribe que las bases de datos constituidas con anterioridad a la entrada en vigencia de la presente ley deberán adecuarse a los términos previstos en ella dentro del plazo de cuarenta y ocho meses, contado desde su entrada en vigencia. Con todo, los titulares de datos podrán ejercer los derechos que les confiere esta ley ante el responsable de datos, a partir de la entrada en vigencia de la ley.

Al iniciarse el estudio de este precepto, **el asesor del Ministerio de Hacienda, señor Godoy**, sugirió a la Comisión reemplazar en la última frase la expresión “la ley” por “esta ley”.

El Presidente de la Comisión, Honorable Senador señor Harboe, connotó que si bien se propone que las bases de datos constituidas con anterioridad a la presente ley deben adecuarse dentro del plazo de 4 años desde que la ley entre en vigencia, los titulares de datos podrán ejercer sus derechos desde el momento en que el mencionado cuerpo legal entre en vigencia.

Consideró que el plazo estipulado es excesivo. Sugirió que dicho término se reduzca a veinticuatro meses. La Comisión concordó con esta proposición.

El señor Presidente de la Comisión declaró cerrado el debate y sometió a votación este artículo, con la enmienda propuesta.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó este artículo, con el cambio indicado.

Artículo tercero

Seguidamente, la Comisión consideró el artículo tercero transitorio del proyecto de ley del Ejecutivo, disposición que prescribe que los reglamentos referidos en la presente ley deberán dictarse dentro de los seis meses siguientes a la fecha de su publicación en el Diario Oficial.

Los representantes del Ejecutivo sugirieron a la Comisión reemplazar la frase “a la fecha de su publicación en el Diario Oficial.” por “desde la entrada en vigencia de esta ley.”.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena estimó necesario que la Agencia de Protección de Datos Personales se encuentre en funcionamiento para la dictación de los reglamentos que establece esta ley.

El asesor del Ministerio de Hacienda, señor Godoy precisó que el hecho que no estén dictados los reglamentos no obsta a que la ley entre en vigencia.

El Presidente de la Comisión, Honorable Senador señor Harboe declaró cerrado el debate.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó este artículo con la enmienda propuesta por el Ejecutivo.

Artículo cuarto

Este precepto transitorio del proyecto de ley del Ejecutivo prescribe que dentro de los sesenta días anteriores a la entrada en vigencia de las modificaciones a la ley N° 19.628, sobre protección de la vida privada, contenida en el artículo primero de la presente ley, el Servicio de Registro Civil e Identificación deberá eliminar el registro de bases de datos personales contemplado en el actual artículo 22 de la ley N° 19.628.

Al iniciarse el estudio de este precepto, se tuvo presente que consultado el Servicio de Registro Civil sobre esta disposición, informó favorablemente el contenido de este precepto.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó este precepto.

Artículo quinto

A continuación, la Comisión examinó el artículo quinto transitorio contenido en el proyecto de ley del Ejecutivo. Esta disposición, faculta al Presidente de la República para que, dentro del plazo de nueve meses contado de la fecha de publicación de esta ley, establezca mediante uno o más decretos con fuerza de ley, expedidos a través del

Ministerio de Hacienda, las normas necesarias para regular las siguientes materias:

En primer lugar, fijar la planta de personal de la Agencia de Protección de Datos Personales y dictar todas las normas necesarias para la adecuada estructuración y operación de ésta. En especial, podrá determinar los grados y niveles de la Escala Única de Sueldos que se asignen a dichas plantas; el número de cargos para cada grado y planta; los requisitos específicos para el ingreso y promoción de dichos cargos; sus denominaciones y los niveles jerárquicos, para efectos de la aplicación de lo dispuesto en el título VI de la ley N° 19.882 y en el artículo 8 de la ley Nº 18.834, cuyo texto refundido, coordinado y sistematizado fue fijado por el decreto con fuerza de ley Nº 29, de 2004, del Ministerio de Hacienda. Asimismo, determinará las normas necesarias para la aplicación de la asignación de modernización de la ley N° 19.553 en su aplicación transitoria.

En segundo lugar, determinar la dotación máxima del personal de la Agencia de Protección de Datos Personales, a cuyo respecto no regirá la limitación establecida en el inciso segundo del artículo 10 del decreto con fuerza de ley Nº 29, de 2004, del Ministerio de Hacienda.

En tercer lugar, determinar la fecha para la entrada en vigencia de las plantas que fije y la iniciación de actividades de la Agencia de Protección de Datos Personales.

Al iniciarse el estudio de esta proposición, se recordó que el Tribunal Constitucional ha señalado que la fijación de los requisitos de ingreso corresponde a una materia que debe ser fijada por ley. Destacó que el artículo 64 de nuestra Carta Fundamental dispone que la autorización que otorga el Congreso Nacional al Presidente de la República, no podrá extenderse a la nacionalidad, la ciudadanía, las elecciones ni al plebiscito, como tampoco a materias comprendidas en las garantías constitucionales o que deban ser objeto de leyes orgánicas constitucionales o de quórum calificado.

Asimismo, se tuvo presente que el artículo 19, número 17 del texto constitucional vigente asegura a toda persona: “La admisión a todas las funciones y empleos públicos, sin otros requisitos que los que impongan la Constitución y las leyes.”.

El asesor del Ministerio de Hacienda señor Braulio Palma expresó que en la mayoría de los servicios públicos, el Ejecutivo fija la Planta y algunos requisitos relacionados con ella, a través, de un decreto con fuerza de ley.

Enfatizó que lo anterior, más que constituir una potestad reglamentaria, viene a ser una delegación legislativa.

Dado lo anterior, sostuvo que en el caso planteado no se vulneraría la garantía del artículo 19, número 17 de la Constitución.

Sobre este punto, se hizo presente que las materias comprendidas en las garantías constitucionales no podían ser delegadas por el Legislativo en el Ejecutivo.

Respecto al número 3), **el Presidente de la Comisión, Honorable Senador señor Harboe**, constató que se faculta al Ejecutivo a determinar la fecha para la entrada en vigencia de las plantas que fije y la iniciación de actividades de la Agencia de Protección de Datos Personales.

Remarcó que se debe consagrar un plazo máximo para ello. Agregó que puede ocurrir que la ley entre en vigencia, que se dicten los reglamentos y que el Ejecutivo determine que la Agencia entrará en vigencia en un plazo muy posterior.

La asesora del Ministerio de Economía, señora Bernardita Piedrabuena consignó que es partidaria de fijar un término de tres meses para que el Ejecutivo cumpla con lo encomendado.

En relación a este último punto, el Ejecutivo hizo llegar a la Comisión una indicación para sustituir el número 3) de este precepto por el siguiente:

3”) Determinar la fecha de entrada en vigencia de las plantas y de iniciación de las actividades de la Agencia de Protección de Datos Personales, la que no podrá exceder de tres meses a la total tramitación del decreto con fuerza de ley que contenga la planta de personal de la Agencia de Protección de Datos Personales.”.

El Presidente de la Comisión, Honorable Senador señor Harboe declaró cerrado el debate.

La Comisión, por la unanimidad de sus miembros presentes, aprobó el artículo quinto transitorio, con las siguientes votaciones:

El número 1), con la enmienda de suprimir la frase “los requisitos específicos para el ingreso y promoción de dichos cargos”, con los votos a favor de los Honorables Senadores señores Araya, Harboe y Larraín. Con la misma votación se aprobó el número 2) de este precepto.

El número 3) de este precepto fue aprobado con los votos a favor de los Honorables Senadores señores Araya, De Urresti, Harboe y Larraín.

Artículo sexto

Seguidamente, la Comisión analizó el artículo sexto transitorio del proyecto de ley del Ejecutivo. Este precepto establece que el Presidente de la República, por decreto expedido por intermedio del Ministerio de Hacienda, conformará el primer presupuesto de la Agencia de Protección de Datos Personales, y transferirá a ella los fondos necesarios para que se cumplan sus funciones, pudiendo al efecto crear, suprimir o modificar los capítulos, asignaciones, ítem y glosas presupuestarias que sean pertinentes.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó sin enmiendas, este artículo.

Artículo séptimo

A continuación, la Comisión trató el artículo séptimo transitorio del proyecto de ley del Ejecutivo. Esta disposición prescribe que dentro de los sesenta días siguientes a la publicación de la presente ley, se deberá convocar al concurso público para el nombramiento del primer director o directora de la Agencia de Protección de Datos Personales, conforme al Sistema de Alta Dirección Pública regulado en la ley N° 19.882. El Presidente de la República podrá nombrar al Director o Directora de la Agencia de Protección de Datos Personales antes de la fecha en que ésta inicie sus actividades, para efectos de la instalación de la misma. En tanto no inicie sus actividades dicha Agencia, la remuneración del Director, grado 1C, de la Escala Única de Sueldos, se financiará con cargo a la Partida del Presupuesto del Ministerio de Hacienda, Capítulo 01, Programa 01.

La Comisión acordó aprobar este precepto con la única enmienda de eliminar la expresión “o Directora” la dos veces que aparece. Adoptó este acuerdo en el entendido de que tal cambio en ningún caso implica que una mujer no pueda desempeñar este cargo. Se tuvo presente que el término legal “director” comprende tanto a hombres como a mujeres.

Se pronunciaron a favor de este precepto, con la enmienda ya indicada, **la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores Araya, Harboe y Larraín.**

Artículo octavo

En seguida, la Comisión analizó el artículo octavo transitorio contenido en el proyecto de ley del Ejecutivo. Esta norma estatuye que los órganos públicos que establezcan un encargado de prevención o delegado de protección de datos personales deberán designar a un funcionario de la dotación vigente del respectivo organismo.

El Honorable Senador señor Larraín sugirió a la Comisión intercale la expresión “para ello”, a continuación del término “designar”.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó el artículo octavo transitorio con la enmienda indicada.

Artículo noveno

Finalmente, la Comisión consideró el artículo noveno transitorio del proyecto de ley del Ejecutivo. Esta norma señala que el mayor gasto que irrogue la aplicación de esta ley en el transcurso del primer año presupuestario de vigencia será financiado con reasignaciones del presupuesto del Ministerio de Hacienda, y en lo que faltare con cargo a recursos del Tesoro Público. Para los años siguientes se estará a lo que indique la Ley de Presupuestos respectiva.

La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Harboe y Larraín, aprobó sin enmiendas esta disposición.

-.-.-

En mérito de los acuerdos precedentemente expuestos, la Comisión de Constitución, Legislación, Justicia y Reglamento tiene el honor proponer la aprobación, en general, del siguiente proyecto de ley:

PROYECTO DE LEY

“Artículo primero. Introdúcense las siguientes modificaciones a la ley Nº 19.628, sobre protección de la vida privada:

1) Reemplázase el artículo 1° por el siguiente:

“Artículo 1°.- Objeto y ámbito de aplicación. La presente ley tiene por objeto regular el tratamiento de los datos personales que realicen las personas naturales o jurídicas, públicas o privadas, con el propósito de asegurar el respeto y protección de los derechos y libertades de las personas naturales que son titulares de estos datos, en particular, el derecho a la vida privada.

Todo tratamiento de datos personales que realice una persona natural o jurídica, incluidos los órganos públicos, cuando no se encuentre regido por una ley especial, quedará sujeto a las disposiciones de esta ley. En los asuntos no regulados en leyes especiales, se aplicarán supletoriamente las normas de esta ley.

El régimen de tratamiento y protección de datos establecidos en esta ley no se aplicará al tratamiento de datos que se realice en el ejercicio de las libertades de emitir opinión y de informar reguladas por las leyes a que se refiere el artículo 19 N° 12 de la Constitución Política de la República. Los medios de comunicación social quedarán sujetos a las disposiciones de esta ley en lo relativo al tratamiento de datos que efectúen con una finalidad distinta a la de opinar e informar.

Tampoco serán aplicables las normas de la presente ley al tratamiento de datos que efectúen las personas naturales en relación con sus actividades personales.

2) Agrégase, antes del artículo 2°, el siguiente epígrafe: “Definiciones.”.

3) Introdúcense las siguientes modificaciones al artículo 2°:

uno) Reemplázanse las letras c), f), g) e i) por las siguientes:

c) Comunicación o transmisión de datos personales: dar a conocer por el responsable de datos, de cualquier forma, datos personales a personas distintas del titular a quien conciernen los datos, sin llegar a cederlos o transferirlos. Las comunicaciones que realice el responsable de datos deben contener información exacta, completa y veraz.

f) Dato personal: cualquier información vinculada o referida a 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, tales 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, excluyendo aquellos casos en que el esfuerzo de identificación sea desproporcionado.

g) Datos personales sensibles: aquellos datos personales que revelen el origen étnico o racial, la afiliación política, sindical o gremial, las convicciones ideológicas o filosóficas, las creencias religiosas, los datos relativos a la salud, al perfil biológico humano, los datos biométricos, y la información relativa a la vida sexual, a la orientación sexual y a la identidad de género de una persona natural.

i) Fuentes de acceso público: todas aquellas bases de datos o conjuntos de datos personales, públicos o privados, cuyo acceso o consulta puede ser efectuada en forma lícita por cualquier persona, siempre que no existan restricciones o impedimentos legales para su acceso o utilización.

dos) Elimínase la letra j), pasando la actual letra k) a ser j) y así sucesivamente.

tres) Sustitúyense las actuales letras l), m), n), ñ) y o), que pasaron a ser k), l), m), n) y ñ), respectivamente, por las siguientes:

k) Proceso de anonimización o disociación: procedimiento en virtud del cual un dato personal no pueden vincularse o asociarse a una persona determinada, ni permitir su identificación, por haberse destruido o eliminado el nexo con la información que vincula, asocia o identifica a esa persona. Un dato anonimizado deja de ser un dato personal.

l) Base de datos personales: conjunto organizado de datos personales, cualquiera sea la forma o modalidad de su creación, almacenamiento, organización y acceso, que permita relacionar los datos entre sí, así como realizar su tratamiento.

m) Responsable de datos o responsable: toda persona natural o jurídica, pública o privada, que decide acerca de los fines y medios del tratamiento de datos personales, con independencia de si los datos son tratados directamente por ella o a través de un tercero mandatario o encargado.

n) Titular de datos o titular: persona natural, identificada o identificable, a quien conciernen o se refieren los datos personales.

ñ) Tratamiento de datos: cualquier operación o conjunto de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, procesar, almacenar, comunicar, transmitir o utilizar de cualquier forma datos personales o conjuntos de datos personales.

cuatro) Agréganse los siguientes literales o), p), q), r), s), t) y u), nuevos:

o) Consentimiento: toda manifestación de voluntad libre, específica, inequívoca e informada, mediante la cual el titular de datos, su representante legal o mandatario, según corresponda, autoriza el tratamiento de los datos personales que le conciernen.

p) Derecho de acceso: derecho del titular de datos a solicitar y obtener del responsable, confirmación acerca de si sus datos personales están siendo tratados por él, acceder a ellos en su caso, y a la información prevista en esta ley.

q) Derecho de rectificación: derecho del titular de datos a solicitar y obtener del responsable, que modifique o complete sus datos personales, cuando están siendo tratados por él, y sean inexactos o incompletos.

r) Derecho de cancelación: derecho del titular de datos a solicitar y obtener del responsable, que suprima o elimine sus datos personales, de acuerdo a las causales previstas en la ley.

s) Derecho de oposición: derecho del titular de datos a solicitar y obtener del responsable, que no se lleve a cabo un tratamiento de datos determinado, de conformidad a las causales previstas en la ley.

t) Derecho a la portabilidad de los datos personales: derecho del titular de datos a solicitar y obtener del responsable, una copia de sus datos personales en un formato electrónico estructurado, genérico y común, que permita ser operado por distintos sistemas, y poder comunicarlos o transferirlos a otro responsable de datos.

u) Registro Nacional de Cumplimiento y Sanciones: registro nacional de carácter público administrado por la Agencia de Protección de Datos Personales, que consigna las sanciones impuestas a los responsables de datos por infracción a la ley, los modelos de prevención de infracciones que implementen los responsables y los programas de cumplimiento debidamente certificados.

4) Sustitúyese el artículo 3º por el siguiente:

Artículo 3.- Principios. El tratamiento de los datos personales se rige por los siguientes principios:

a) Principio de licitud del tratamiento. Los datos personales sólo pueden tratarse con sujeción a la ley.

b) Principio de finalidad. Los datos personales deben ser recolectados con fines específicos, explícitos y lícitos. El tratamiento de los datos personales debe limitarse al cumplimiento de estos fines.

En aplicación de este principio, no se pueden tratar los datos personales con fines distintos a los informados al momento de la recolección, salvo que el tratamiento sea para fines compatibles con los autorizados originalmente; exista una relación contractual o pre contractual entre el titular y el responsable que justifique el tratamiento de los datos con una finalidad distinta; el titular otorgue nuevamente su consentimiento; los datos provengan de fuentes de acceso público, y cuando lo disponga la ley.

c) Principio de proporcionalidad. Los datos personales que se traten deben limitarse a aquellos que resulten necesarios en relación con los fines del tratamiento.

Los datos personales deben ser conservados sólo por el período de tiempo que sea necesario para cumplir con los fines del tratamiento, luego de lo cual deben ser cancelados o anonimizados. Un período de tiempo mayor requiere autorización legal o consentimiento del titular.

d) Principio de calidad. Los datos personales deben ser exactos, completos y actuales, en relación con los fines del tratamiento.

e) Principio de responsabilidad. Quienes realicen tratamiento de los datos personales serán legalmente responsables del cumplimiento de los principios, obligaciones y deberes de conformidad a la ley.

f) Principio de seguridad. En el tratamiento de los datos personales, el responsable debe garantizar estándares adecuados de seguridad, protegiéndolos contra el tratamiento no autorizado, pérdida, filtración, daño o destrucción y, aplicando para ello, las medidas técnicas u organizativas apropiadas.

g) Principio de transparencia e información. Las políticas y las prácticas sobre el tratamiento de los datos personales deben estar permanentemente accesibles y a disposición de cualquier interesado de manera precisa, clara, inequívoca y gratuita.

El responsable debe adoptar las medidas adecuadas y oportunas para facilitar al titular el acceso a toda la información que señala esta ley, así como cualquier otra comunicación relativa al tratamiento que realiza.

h) Principio de confidencialidad. El responsable de datos personales y quienes tengan acceso a ellos deberán guardar secreto o confidencialidad acerca de los mismos. El responsable establecerá controles y medidas adecuadas para preservar el secreto o confidencialidad. Este deber subsiste aún después de concluida la relación con el titular.

5) Reemplázase el Título I por el siguiente:

“Título I
De los derechos del titular de datos personales

Artículo 4º.- Derechos del titular de datos. Toda persona actuando por sí o a través de su representante legal o mandatario, según corresponda, tiene derecho de acceso, rectificación, cancelación, oposición y portabilidad de sus datos personales, de conformidad a la presente ley.

Tales derechos son personales, intransferibles e irrenunciables y no pueden limitarse por ningún acto o convención.

En caso de fallecimiento del titular de datos, los derechos que reconoce esta ley pueden ser ejercidos por sus herederos.

Artículo 5º.- Derecho de acceso. El titular de datos tiene derecho a solicitar y obtener del responsable, confirmación acerca de si los datos personales que le conciernen están siendo tratados por él, y en tal caso, acceder a dichos datos y a la siguiente información:

a) Los datos tratados y su origen.

b) La finalidad o finalidades del tratamiento.

c) Las categorías, clases o tipos de destinatarios a los que se han comunicado o cedido los datos o se prevé comunicar o ceder, según corresponda, y

d) El período de tiempo durante el cual los datos serán tratados.

El responsable no estará obligado a entregar la información solicitada por el titular en los siguientes casos:

i. Cuando el titular ya disponga de la información requerida.

ii. Cuando su comunicación resulte imposible o su entrega exija un esfuerzo desproporcionado.

iii. Cuando su entrega imposibilite u obstaculice gravemente un tratamiento de datos con fines históricos, estadísticos o científicos, para estudios o investigaciones que atiendan fines de interés público o vayan en beneficio de la salud humana, y

iv. Cuando lo disponga expresamente la ley.

Artículo 6º. Derecho de rectificación. El titular de datos tiene derecho a solicitar y obtener del responsable, la rectificación de los datos personales que le conciernen y que están siendo tratados por él, cuando sean inexactos, desactualizados o incompletos.

La rectificación y su contenido serán públicas y deberán difundirse, cuando así lo requiera el titular y sea necesario para los fines del tratamiento realizado.

Artículo 7°.- Derecho de cancelación. El titular de datos tiene derecho a solicitar y obtener del responsable la cancelación o supresión de los datos personales que le conciernen, en los siguientes casos.

a) Cuando los datos no resulten necesarios en relación con los fines del tratamiento para el cual fueron recogidos.

b) Cuando el titular haya revocado su consentimiento para el tratamiento y éste no tenga otro fundamento legal.

c) Cuando los datos hayan sido obtenidos o tratados ilícitamente por el responsable.

d) Cuando se trate de datos caducos.

e) Cuando los datos deban suprimirse para el cumplimiento de una sentencia judicial o de una obligación legal, y

f) Cuando el titular haya ejercido su derecho de oposición de conformidad al artículo siguiente y no existan otro fundamento legal para su tratamiento.

No procede la cancelación cuando el tratamiento sea necesario:

i. Para ejercer el derecho a las libertades de emitir opinión y de informar.

ii. Para el cumplimiento de una obligación legal o la ejecución de un contrato suscrito entre el titular y el responsable.

iii. Por razones de interés público, especialmente en el ámbito de la salud pública.

iv. Para tratamientos con fines históricos, estadísticos o científicos y para estudios o investigaciones que atiendan fines de interés público, y

v. Para la formulación, ejercicio o defensa de una reclamación administrativa o judicial.

Artículo 8°.- Derecho de Oposición. El titular de datos tiene derecho a oponerse ante el responsable a que se realice un tratamiento específico o determinado de los datos personales que le conciernan, en los siguientes casos:

a) Si el tratamiento afecta sus derechos y libertades fundamentales.

b) Si el tratamiento se realiza exclusivamente con fines de mercadotecnia o marketing directo de bienes, productos o servicios, salvo que exista un contrato entre el titular y el responsable.

c) Si el titular de los datos hubiere fallecido. En este caso, la oposición deberá ser formulada por los herederos, y

d) Si el tratamiento se realiza respecto de datos obtenidos de una fuente de acceso público y no exista otro fundamento legal para su tratamiento.

No procederá la oposición al tratamiento en los siguientes casos:

i. Cuando sea necesario para ejercer el derecho a las libertades de emitir opinión y de informar.

ii. Cuando existan razones de interés público, especialmente en el ámbito de la salud pública.

iii. Cuando se realice con fines históricos, estadísticos o científicos y para estudios o investigaciones que atiendan fines de interés público, y

iv. Cuando se requiera para la formulación, ejercicio o defensa de una reclamación administrativa o judicial.

Artículo 8° bis.- Derecho de oposición a valoraciones personales automatizadas. El titular de datos tiene derecho a oponerse a que el responsable adopte decisiones que le afecten significativamente en forma negativa o le produzcan efectos jurídicos adversos, basadas únicamente en el tratamiento automatizado de sus datos personales, incluida la elaboración de perfiles.

El titular no podrá ejercer este derecho de oposición en los siguientes casos:

a) Cuando la decisión del responsable sea necesaria para la celebración o ejecución de un contrato entre el titular y el responsable;

b) Cuando exista consentimiento previo y expreso del titular, y

c) Cuando lo disponga la ley.

En los casos de las letras a) y b) del inicio anterior, el responsable deberá adoptar las medidas necesarias para asegurar los derechos del titular, en particular el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a solicitar la revisión de la decisión.

Artículo 9º.- Derecho a la portabilidad de los datos personales. El titular de datos tiene derecho a solicitar y recibir del responsable, una copia de los datos personales que le conciernen de manera estructurada, en un formato genérico y de uso común, que permita ser operado por distintos sistemas y, a comunicarlos o transferirlos a otro responsable de datos, cuando concurran las siguientes circunstancias o requisitos:

a) El titular haya entregado sus datos personales directamente al responsable. No procede el ejercicio de este derecho respecto de la información inferida, derivada, creada, generada u obtenida a partir del análisis o tratamientos realizados por el responsable.

b) Se trate de un volumen relevante de datos y sean tratados en forma automatizada, y

c) Exista consentimiento del titular para el tratamiento o se requiera para la ejecución o cumplimiento de un contrato.

El responsable debe utilizar los medios más expeditos, menos onerosos y sin poner trabas u obstáculos para el ejercicio de este derecho.

El responsable también debe comunicar al titular de manera clara y precisa las medidas necesarias para recuperar sus datos personales y especificar las características técnicas para llevar a cabo estas operaciones.

Artículo 10.- Forma y medios de ejercer los derechos del titular de datos. Los derechos reconocidos en esta ley se ejercen por el titular ante el responsable de datos. Si los datos personales del titular son tratados por diversos responsables, el titular puede ejercer sus derechos ante cualquiera de ellos.

Los responsables de datos deberán implementar mecanismos y herramientas tecnológicas que permitan que el titular ejerza sus derechos en forma expedita, ágil y eficaz. Los medios dispuestos por el responsable deben ser sencillos en su operación.

El ejercicio de los derechos de rectificación, cancelación y oposición siempre serán gratuitos para el titular. El derecho de acceso también se ejercerá en forma gratuita, al menos trimestralmente.

El responsable de datos sólo puede exigir el pago de los costos directos en que incurra, cuando el titular ejerza su derecho de

acceso más de una vez en el trimestre o cuando ejerza el derecho a la portabilidad.

La Agencia de Protección de Datos Personales a través de una norma de carácter general establecerá los parámetros y mecanismos para determinar los costos indicados en el inciso anterior.

La Agencia de Protección de Datos Personales velará por el efectivo ejercicio y cumplimiento de los derechos que esta ley reconoce al titular de datos.

Artículo 11.- Procedimiento ante el responsable de datos. Para ejercer los derechos que le reconoce esta ley, el titular deberá presentar una solicitud o requerimiento escrito ante el responsable, dirigido a la dirección de correo electrónico establecida para este fin, a través de un formulario de contacto o un medio electrónico equivalente. La solicitud deberá contener, a lo menos, las siguientes menciones:

a) Individualización del titular y de su representante legal o mandatario, según corresponda y autenticación de su identidad de acuerdo a los procedimientos, formas y modalidades que establezca la Agencia de Protección de Datos Personales.

b) Indicación de un domicilio o una dirección de correo electrónico o de otro medio equivalente para comunicar la respuesta.

c) Identificación de los datos personales o del tratamiento determinado, respecto de los cuales se ejerce el derecho correspondiente.

d) En las solicitudes de rectificación, el titular deberá indicar las modificaciones o actualizaciones precisas a realizar y acompañar, en su caso, los antecedentes que las sustenten. Cuando se trate de solicitudes de cancelación, el titular deberá indicar la causal invocada y acompañar los antecedentes que la sustenten, si correspondiere. Para las solicitudes de oposición, el titular deberá indicar la causal invocada y en el caso de la letra a) del artículo 8°, deberá fundamentar brevemente su petición, podrá igualmente acompañar los antecedentes que estime procedentes. En el caso del derecho de acceso, bastará con la individualización del titular, y

e) Cualquier otro antecedente que facilite la localización de los datos personales.

Recibida la solicitud el responsable deberá acusar recibo de ella y pronunciarse a más tardar dentro de los 15 días hábiles siguientes a la fecha de ingreso.

El responsable deberá responder por escrito al titular a su domicilio o la dirección de correo electrónico fijada por éste. Cuando la respuesta se entregue por otro medio electrónico, el responsable debe almacenar los respaldos que le permitan demostrar la transmisión y recepción de la respuesta, su fecha y el contenido íntegro de ella.

En caso de denegación total o parcial de la solicitud, el responsable deberá fundar su decisión indicando la causa invocada y los antecedentes que la justifican. En esta misma oportunidad el responsable debe señalar al titular que dispone de un plazo de 15 días hábiles para formular una reclamación ante la Agencia de Protección de Datos Personales, de acuerdo al procedimiento establecido en el artículo 45.

Transcurrido el plazo de 15 días hábiles al que hace referencia el inciso segundo anterior, sin que haya respuesta del responsable, el titular podrá formular directamente una reclamación ante la Agencia de Protección de Datos Personales, en los mismos términos del inciso anterior.

Cuando se formule una solicitud de rectificación, cancelación u oposición, el titular tendrá derecho a solicitar y obtener del responsable el bloqueo temporal de sus datos o del tratamiento que realice, según corresponda. La solicitud de bloqueo temporal deberá ser fundada y el responsable deberá responder al requerimiento dentro de los dos días hábiles siguientes a su recepción. En tanto no resuelva esta solicitud, el responsable no podrá tratar los datos del titular que forman parte del requerimiento. En caso de rechazo el responsable deberá fundar su respuesta y comunicar en forma electrónica su decisión a la Agencia de Protección de Datos Personales. El titular podrá reclamar de esta decisión ante la Agencia de Protección de Datos Personales, aplicándose lo dispuesto en la letra i) del artículo 45.

La rectificación, cancelación u oposición al tratamiento de los datos se aplicarán sólo respecto de los responsables a quienes se les haya formulado la solicitud.

6) Reemplázase el Título II por el siguiente:

“Título II
Del tratamiento de los datos personales y de las categorías especiales de datos

Párrafo Primero

Del consentimiento del titular, de las obligaciones y deberes del responsable y del tratamiento de datos en general

Artículo 12.- Regla general del tratamiento de datos. Es lícito el tratamiento de los datos personales que le conciernen al titular, cuando otorgue su consentimiento para ello.

El consentimiento del titular debe ser libre, informado y específico en cuanto a su finalidad o finalidades. El consentimiento debe manifestarse de manera inequívoca, mediante una declaración verbal, escrita o expresada a través de un medio electrónico equivalente, o mediante un acto afirmativo que dé cuenta con claridad de la voluntad del titular.

Cuando el consentimiento lo otorgue un mandatario, éste deberá encontrarse expresamente premunido de esta facultad.

El titular puede revocar el consentimiento otorgado en cualquier momento y sin expresión de causa, utilizando medios similares o equivalentes a los empleados para su otorgamiento. La revocación del consentimiento no tendrá efectos retroactivos.

Los medios utilizados para el otorgamiento o la revocación del consentimiento deben ser expeditos, fidedignos, gratuitos y estar permanentemente disponibles para el titular.

El consentimiento no se considerará una base jurídica suficiente para la validez del tratamiento de datos, cuando exista un desequilibrio ostensible entre la posición del titular y el responsable.

Corresponde al responsable probar que el tratamiento de datos realizado contó con el consentimiento del titular.

Artículo 13.- Otras fuentes de licitud del tratamiento de datos. Es lícito el tratamiento de datos personales, sin el consentimiento del titular, en los siguientes casos:

a) Cuando los datos han sido recolectados de una fuente de acceso público y su tratamiento esté relacionado con los fines para los cuales fueron entregados o recogidos.

b) Cuando el tratamiento esté referido a datos relativos a obligaciones de carácter económico, financiero, bancario o comercial y se realice de conformidad con las normas del Título III de esta ley.

c) Cuando el tratamiento sea necesario para la ejecución o el cumplimiento de una obligación legal o lo disponga la ley.

d) Cuando el tratamiento de datos sea necesario para la celebración o ejecución de un contrato entre el titular y el responsable, o para la ejecución de medidas precontractuales adoptadas a solicitud del titular.

e) Cuando el tratamiento sea necesario para la satisfacción de intereses legítimos del responsable o de un tercero, siempre que con ello no se afecten los derechos y libertades del titular.

f) Cuando el tratamiento de datos sea necesario para la formulación, ejercicio o defensa de un derecho ante los tribunales de justicia.

El responsable deberá acreditar la licitud del tratamiento de datos.

Artículo 14.- Obligaciones del responsable de datos. El responsable de datos, sin perjuicio de las demás disposiciones previstas en esta ley, tiene las siguientes obligaciones:

a) Informar y poner a disposición del titular, de manera expedita y cuando le sean requeridos, los antecedentes que acrediten la licitud del tratamiento de datos que realiza.

b) Asegurar que los datos personales se recojan de fuentes de acceso lícitas con fines específicos, explícitos y lícitos, y que su tratamiento se limite al cumplimiento de estos fines.

c) Comunicar o ceder, en conformidad a las disposiciones de esta ley, información exacta, completa y actual.

d) Cancelar o anonimizar los datos personales del titular cuando fueron obtenidos para la ejecución de medidas precontractuales, y

e) Cumplir con los demás principios que rigen el tratamiento de los datos personales previstos en esta ley.

Artículo 14 bis.- Deber de secreto o confidencialidad. El responsable de datos está obligado a mantener secreto o confidencialidad acerca de los datos personales que conciernan a un titular, salvo aquellos que provengan de fuentes de acceso público o cuando el titular los hubiere hecho manifiestamente públicos. Este deber subsiste aún después de concluida la relación con el titular.

El deber de secreto o confidencialidad no obsta a las comunicaciones o cesiones de datos que deba realizar el responsable en conformidad a la ley, y al cumplimiento de la obligación de dar acceso al titular e informar el origen de los datos, cuando esta información le sea requerida por el titular o por un órgano público dentro del ámbito de sus competencias legales.

El responsable debe adoptar las medidas necesarias con el objeto que sus dependientes o las personas naturales o jurídicas que ejecuten operaciones de tratamiento de datos bajo su responsabilidad, cumplan el deber de secreto o confidencialidad establecidos en este artículo.

Quedan sujetas a la obligación de secreto o confidencialidad las personas e instituciones y sus dependientes, que en cumplimiento de una obligación legal han remitido información a un organismo público sujeto al régimen de excepciones establecido en el artículo 24, en cuanto al requerimiento y al hecho de haber remitido dicha información.

Artículo 14 ter.- Deber de información y transparencia. El responsable de datos debe mantener permanentemente a disposición del público, en su sitio web o en cualquier otro medio de información equivalente, al menos, la siguiente información:

a) La política de tratamiento de datos personales que haya adoptado, la fecha y versión de la misma.

b) La individualización del responsable de datos y su representante legal y la identificación del encargado de prevención, si existiere.

c) La dirección de correo electrónico, el formulario de contacto o la identificación del medio tecnológico equivalente a través del cual se le notifican las solicitudes que realicen los titulares.

d) Las categorías, clases o tipos de datos que trata; la descripción genérica del universo de personas que comprenden sus bases de datos; los destinatarios a los que se prevé comunicar o ceder los

datos, las finalidades de los tratamientos que realiza y los tratamientos que se basan en la satisfacción de intereses legítimos.

e) La política y las medidas de seguridad adoptadas para proteger las bases de datos personales que administra.

f) El derecho que le asiste al titular para solicitar ante el responsable, acceso, rectificación, cancelación, oposición y portabilidad de sus datos personales, de conformidad a la ley, y

g) El derecho que le asiste al titular de recurrir ante la Agencia de Protección de Datos Personales, en caso que el responsable rechace o no responda oportunamente las solicitudes que le formule.

Artículo 14 quater.- Deber de adoptar medidas de seguridad. El responsable de datos debe adoptar las medidas necesarias para resguardar el cumplimiento del principio de seguridad establecido en esta ley, considerando el estado actual de la técnica y los costos de aplicación, junto con la naturaleza, alcance, contexto y fines del tratamiento, así como la probabilidad de los riesgos y la gravedad de sus efectos en relación con el tipo de datos tratados. Las medidas aplicadas por el responsable deben asegurar la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas de tratamiento de datos.

Si las bases de datos que opera el responsable tienen distintos niveles de criticidad, deberá adoptar las medidas de seguridad que correspondan al nivel más alto.

Ante la ocurrencia de un incidente de seguridad, y en caso de controversia judicial o administrativa, corresponderá al responsable acreditar la existencia y el funcionamiento de las medidas de seguridad adoptadas en base a los niveles de criticidad y a la tecnología disponible.

Artículo 14 quinquies.- Deber de reportar las vulneraciones a las medidas de seguridad. El responsable de datos deberá reportar a la Agencia de Protección de Datos Personales, por los medios más expeditos posibles y sin dilaciones indebidas, las vulneraciones a las medidas de seguridad que ocasionen la destrucción, filtración, pérdida o alteración accidental o ilícita de los datos personales que trate o la comunicación o acceso no autorizados a dichos datos, cuando exista un riesgo razonable que con ocasión de estos incidentes se genere un perjuicio o afectación para los titulares.

El responsable de datos deberá registrar estas comunicaciones, describiendo la naturaleza de las vulneraciones sufridas, sus efectos, las categorías de datos y el número aproximado de titulares afectados y las medidas adoptadas para gestionarlas y precaver incidentes futuros.

Cuando dichas vulneraciones se refieran a datos personales sensibles o datos relativos a obligaciones de carácter económico, financiero, bancario o comercial, el responsable deberá también efectuar esta comunicación a los titulares de estos datos. Esta comunicación deberá realizarse en un lenguaje claro y sencillo, singularizando los datos afectados, las posibles consecuencias de las vulneraciones de seguridad y las medidas de solución o resguardo adoptadas. La notificación se deberá realizar a cada titular afectado y si ello no fuere posible, se realizará mediante la difusión o publicación de un aviso en un medio de comunicación social masivo y de alcance nacional.

Artículo 14 sexies.- Diferenciación de estándares de cumplimiento. Los estándares o condiciones mínimas que se impongan al responsable de datos para el cumplimiento de los deberes de información y de seguridad establecidos en los artículos 14 ter y 14 quáter, respectivamente, serán determinados considerando si el responsable es una persona natural o jurídica, el tamaño de la entidad o empresa de acuerdo a las categorías establecidas en el artículo segundo de la ley N° 20.416, que fija normas especiales para las empresas de menor tamaño, y el volumen y las finalidades de los datos personales que trata.

Los estándares de cumplimiento y las medidas diferenciadas serán especificadas en un reglamento expedido por el Ministerio de Hacienda y suscrito por el Ministro de Economía, Fomento y Turismo, previo informe de la Agencia de Protección de Datos Personales.

La Agencia de Protección de Datos Personales al definir los parámetros y mecanismos para determinar los costos derivados del ejercicio de los derechos de acceso y portabilidad de acuerdo al artículo diez de esta ley, deberá considerar también el volumen de datos, la naturaleza jurídica y el tamaño de la entidad o empresa que tenga la calidad de responsable de datos.

Artículo 15.- Cesión de datos personales. Los datos personales podrán ser cedidos con el consentimiento del titular y para el cumplimiento de los fines del tratamiento. También se podrán ceder los datos personales cuando la cesión sea necesaria para la ejecución de un contrato en que es parte el titular; cuando exista un interés legítimo del

cedente o del cesionario, en los términos previstos en la letra e) del artículo 13, y cuando lo disponga la ley.

En caso que el consentimiento otorgado por el titular al momento de realizarse la recolección de los datos personales no haya considerado la cesión de los mismos, éste debe recabarse antes que se produzca, considerándose para todos los efectos legales como una nueva operación de tratamiento.

La cesión de datos deberá constar por escrito o a través de cualquier medio electrónico idóneo. En ella se deberá individualizar a las partes, los datos que son objeto de la cesión, las finalidades previstas para el tratamiento y los demás antecedentes o estipulaciones que acuerden el cedente y el cesionario.

El tratamiento de los datos personales cedidos deberá realizarse por el cesionario de conformidad a las finalidades establecidas en el contrato de cesión.

Una vez perfeccionada la cesión, el cesionario adquiere la condición de responsable de datos para todos los efectos legales. El cedente, por su parte, también mantiene la calidad de responsable de datos, respecto de las operaciones de tratamiento que continúe realizando.

Si se verifica una cesión de datos sin contar con el consentimiento del titular, siendo éste necesario, la cesión será nula, debiendo el cesionario suprimir todos los datos recibidos, sin perjuicio de las responsabilidades legales que correspondan.

Artículo 15 bis.- Tratamiento de datos a través de un tercero mandatario o encargado. El responsable puede efectuar el tratamiento de datos en forma directa o a través de un tercero mandatario o encargado. En este último caso, el tercero mandatario o encargado realiza el tratamiento de datos personales conforme al encargo y a las instrucciones que le imparta el responsable, quedándole prohibido su tratamiento, cesión o entrega para un objeto distinto del convenido con el responsable.

Si el tercero mandatario o encargado trata, cede o entrega los datos con un objeto distinto del encargo convenido, se le considerará como responsable de datos para todos los efectos legales, debiendo responder por las infracciones en que incurra y solidariamente por los daños que ocasione, sin perjuicio de las responsabilidades contractuales que le correspondan frente al mandante o responsable de datos.

El tratamiento de datos a través de un tercero mandatario o encargado se regirá por el contrato celebrado entre el responsable y el encargado, con arreglo a la legislación vigente. En el contrato se deberá establecer el objeto del encargo, la duración del mismo, la finalidad del tratamiento, el tipo de datos personales tratados, las categorías de titulares a quienes conciernen los datos, y los derechos y obligaciones de las partes. La Agencia de Protección de Datos Personales en su página web pondrá a disposición del público modelos tipo de contratos.

El tercero mandatario o encargado deberá cumplir con lo dispuesto en los artículos 14 bis, 14 quater y 14 quinquies.

Cumplida la prestación del servicio de tratamiento por parte del tercero mandatario o encargado, los datos que obran en su poder deben ser cancelados o devueltos al responsable de datos, según corresponda.

Las personas naturales o jurídicas que presten servicios de infraestructura, plataforma, software u otros servicios para el almacenamiento o procesamiento de los datos, o para facilitar enlaces o instrumentos de búsqueda, no tendrán la calidad de responsable de datos para los efectos de esta ley, salvo que tomen decisiones acerca de los medios y fines del tratamiento de datos, en cuyo caso responderán de acuerdo a las normas previstas en esta ley para los responsables de datos, sin perjuicio de las demás responsabilidades y sanciones que les puedan caber por incumplimiento de contratos o infracciones legales.

Artículo 15 ter.- Tratamiento automatizado de grandes volúmenes de datos.- El responsable de datos podrá establecer procedimientos automatizados de tratamiento y transferencia de grandes volúmenes de datos, siempre que los mismos cautelen los derechos del titular y el tratamiento guarde relación con las finalidades de las personas o entidades participantes.

Párrafo Segundo
Del tratamiento de los datos personales sensibles

Artículo 16.- Regla general para el tratamiento de datos personales sensibles. El tratamiento de los datos personales sensibles sólo puede realizarse cuando el titular a quien conciernen estos datos manifiesta su consentimiento en forma expresa, otorgado a través de una declaración escrita, verbal o por un medio tecnológico equivalente.

Es lícito el tratamiento de datos personales sensibles, sin el consentimiento del titular, en los siguientes casos:

a) Cuando el tratamiento se refiere a datos personales sensibles que el titular ha hecho manifiestamente públicos y su tratamiento esté relacionado con los fines para los cuales fueron publicados.

b) Cuando el tratamiento se basa en un interés legítimo realizado por una persona jurídica de derecho público o de derecho privado que no persiga fines de lucro y se cumplan las siguientes condiciones:

i.- Su finalidad sea política, filosófica, religiosa, cultural, sindical o gremial;

ii.- El tratamiento que realice se refiera exclusivamente a sus miembros o afiliados;

iii.- El tratamiento de datos tenga por objeto cumplir las finalidades específicas de la institución;

iv.- La persona jurídica otorgue las garantías necesarias para evitar un uso o tratamiento no autorizado de los datos, y

v.- Los datos personales no se comuniquen o cedan a terceros.

Cumpliéndose estas condiciones, la persona jurídica no requerirá el consentimiento del titular para tratar sus datos, incluidos los datos personales sensibles. En caso de duda o controversia administrativa o judicial, el responsable de datos deberá acreditar su concurrencia.

Cuando un integrante de la persona jurídica deje de pertenecer a ella, sus datos deberán ser anonimizados o cancelados.

c) Cuando el tratamiento de los datos personales, incluidos los datos relativos a la salud del titular, resulte indispensable para salvaguardar la vida, salud o integridad física o psíquica del titular o de otra persona o, cuando el titular se encuentre física o jurídicamente impedido de otorgar su consentimiento. Una vez que cese el impedimento, el responsable debe informar detalladamente al titular los datos que fueron tratados y las operaciones específicas de tratamiento que fueron realizadas.

d) Cuando el tratamiento de los datos sea necesario para la formulación, ejercicio o defensa de un derecho ante los tribunales de justicia.

e) Cuando el tratamiento de datos sea necesario para el ejercicio de derechos y el cumplimiento de obligaciones del responsable o del titular de datos, en el ámbito laboral o de seguridad social, y se realice en el marco de la ley.

f) Cuando el tratamiento de datos personales sensibles lo autorice o mandate expresamente la ley.

Artículo 16 bis.- Datos personales relativos a la salud. Cumpliéndose lo dispuesto en el artículo 16, los datos personales relativos a la salud del titular sólo pueden ser tratados en los siguientes casos:

a) Cuando sea necesario para el diagnóstico de una enfermedad o para la determinación de un tratamiento médico, siempre que el diagnóstico o el tratamiento, según corresponda, se realicen por un establecimiento de salud o por un profesional de la salud.

b) Cuando exista una urgencia médica o sanitaria.

c) Cuando se deba calificar el grado de dependencia o discapacidad de una persona.

d) Cuando resulte indispensable para la ejecución o cumplimiento de un contrato cuyo objeto o finalidad exija tratar datos relativos a la salud del titular.

e) Cuando sean utilizados con fines históricos, estadísticos o científicos, para estudios o investigaciones que atiendan fines de interés público o vayan en beneficio de la salud humana, o para el desarrollo de productos o insumos médicos que no podrían desarrollarse de otra manera.

f) Cuando el tratamiento de los datos sea necesario para la formulación, ejercicio o defensa de un derecho ante los tribunales de justicia.

g) Cuando la finalidad del tratamiento quede expresamente establecida en la ley.

El resultado de los estudios e investigaciones científicas que utilicen datos personales relativos a la salud puede ser publicado o difundido libremente, debiendo previamente anonimizarse los datos que se publiquen.

Artículo 16 ter.- Datos personales biométricos. El responsable que trate datos personales biométricos, tales como la huella digital, el iris, los rasgos de la mano o faciales y la voz, deberá proporcionar al titular la siguiente información específica:

a) La identificación del sistema biométrico usado;

b) La finalidad específica para la cual los datos recolectados por el sistema biométrico serán utilizados;

c) El período durante el cual los datos biométricos serán utilizados, y

d) La forma en que el titular puede ejercer sus derechos.

Un reglamento expedido por el Ministerio de Hacienda, previo informe de la Agencia de Protección de Datos personales, regulará la forma y los procedimientos que se deben utilizar para la implementación de los sistemas biométricos.

Artículo 16 quater.- Datos personales relativos al perfil biológico humano. Cumpliéndose lo dispuesto en el artículo 16, el responsable sólo podrá realizar el tratamiento de los datos personales relativos al perfil biológico del titular, tales como los datos genéticos, protéomicos o metabólicos, para los siguientes fines:

a) Realizar diagnósticos médicos.

b) Prestar asistencia médica o sanitaria en caso de urgencia.

c) Efectuar estudios o investigaciones científicas, médicas o epidemiológicas que vayan en beneficio de la salud humana o investigaciones antropológicas, arqueológicas o de medicina forense.

d) Ejercer un derecho ante los tribunales o cumplir resoluciones judiciales.

e) Los expresamente establecidos en la ley.

Queda prohibido el tratamiento y la cesión de los datos relativos al perfil biológico de un titular y las muestras biológicas asociadas a una persona identificada o identificable, incluido el almacenamiento del material biológico, cuando los datos o muestras han sido

recolectados en el ámbito laboral, educativo, deportivo, social, de seguros, de seguridad o identificación, salvo que la ley expresamente autorice su tratamiento en casos calificados.

Los prestadores institucionales de salud, sean públicos o privados, que requieren tratar datos personales relativos al perfil biológico humano dentro del marco de las funciones que les señala el Código Sanitario o la ley Nº 20.120 y su normativa complementaria, deben adoptar y mantener los más altos estándares de control, seguridad y resguardo de esta información y de las muestras biológicas recolectadas.

El resultado de los estudios e investigaciones científicas que utilicen datos personales relativos al perfil biológico humano puede ser publicado o difundido libremente, debiendo previamente anonimizarse los datos que se publiquen.

Párrafo Tercero
Del tratamiento de categorías especiales de datos personales

Artículo 16 quinquies.- Datos personales relativos a los niños, niñas y adolescentes. El tratamiento de los datos personales que conciernen a los niños, niñas y adolescentes, sólo puede realizarse atendiendo al interés superior de éstos y al respeto de su autonomía progresiva.

Cumpliéndose la exigencia establecida en el inciso anterior, para tratar los datos personales de los niños y niñas se requiere el consentimiento otorgado por sus padres o representantes legales o por quien tiene a su cargo el cuidado personal del niño o niña, salvo que expresamente lo autorice o mandate la ley.

Los datos personales de los adolescentes se podrán tratar de acuerdo a las normas de autorización previstas en esta ley para los adultos, salvo lo dispuesto en el inciso siguiente.

Los datos personales sensibles de los adolescentes menores de 16 años, sólo se podrán tratar con el consentimiento otorgado por sus padres o representantes legales o quien tiene a su cargo el cuidado personal del menor, salvo que expresamente lo autorice o mandate la ley.

Para los efectos de esta ley, se consideran niños o niñas a los menores de catorce años, y adolescentes, a los mayores de catorce y menores de dieciocho años.

Constituye una obligación especial de los establecimientos educacionales y de todas las personas o entidades públicas o privadas que traten o administren datos personales de niños, niñas y adolescentes, incluido quienes ejercen su cuidado personal, velar por el uso lícito y la protección de la información personal que concierne a los niños, niñas y adolescentes.

Artículo 16 sexies.- Datos personales con fines históricos, estadísticos, científicos y de estudios o investigaciones. Se entiende que existe un interés legítimo en el tratamiento de datos personales que realicen las personas naturales o jurídicas, públicas o privadas, incluidos los organismos públicos, cuando el tratamiento se realiza exclusivamente con fines históricos, estadísticos, científicos y para estudios o investigaciones que atiendan fines de interés público.

Los responsables de datos deberán adoptar y acreditar que ha cumplido con todas las medidas de calidad y seguridad necesarias para resguardar que los datos se utilicen exclusivamente para tales fines. Cumplidas estas condiciones, el responsable podrá almacenar y utilizar los datos por un período indeterminado de tiempo.

Los responsables que hayan tratado datos personales exclusivamente con estas finalidades podrán efectuar publicaciones con los resultados y análisis obtenidos, debiendo previamente adoptar las medidas necesarias para anonimizar los datos que se publiquen.

Artículo 16 septies.- Datos de geolocalización. El tratamiento de los datos personales de geolocalización del titular se podrá realizar bajo las mismas bases de licitud establecidas en los artículos 12 y 13 de esta ley.

El titular de datos deberá ser informado de manera clara, suficiente y oportuna, del tipo de datos de geolocalización que serán tratados, de la finalidad y duración del tratamiento y si los datos se comunicarán o cederán a un tercero para la prestación de un servicio con valor añadido.”.

7) Reemplázase en el artículo 17 la frase “banco de datos” por la expresión: “base de datos” todas las veces que aparece en el texto.

8) Modifícase el artículo 19 de la siguiente forma:

a) Reemplázase en el inciso primero el número “12”, precedido de la palabra “artículo, por el número “4º”.

b) Reemplázase la frase “banco de datos” por la expresión “base de datos” todas las veces que aparece en el texto.

c) Sustitúyase en el inciso final la frase “de acuerdo a lo previsto en el artículo 16” por la frase “de conformidad a lo dispuesto en el Título VII de esta ley.”

9) Reemplázase el Título IV por el siguiente:

“Título IV
Del tratamiento de datos personales por los órganos públicos

Artículo 20.- Regla general del tratamiento de datos por órganos públicos. Es lícito el tratamiento de los datos personales que efectúan los órganos públicos cuando se realiza para el cumplimiento de sus funciones legales, dentro del ámbito de sus competencias, de conformidad a las normas establecidas en la ley, y a las disposiciones previstas en este Título. En esas condiciones, los órganos públicos actúan como responsables de datos y no requieren el consentimiento del titular para tratar sus datos personales.

Artículo 21.- Principios y normas aplicables al tratamiento de datos de los órganos públicos. El tratamiento de los datos personales que realicen los órganos públicos se rige por los principios establecidos en el artículo 3° y los principios de coordinación, eficiencia, transparencia y publicidad.

En virtud del principio de coordinación, los organismos públicos deben alcanzar un alto grado de interoperabilidad y coherencia, de modo de evitar contradicciones en la información almacenada y reiteración de requerimientos de información o documentos a los titulares de datos. Conforme al principio de eficiencia, se debe evitar la duplicación de procedimientos y trámites entre los organismos públicos, y entre éstos y los titulares de la información. De acuerdo con los principios de transparencia y publicidad, los organismos públicos deben dar acceso a la información que tengan a su disposición, resguardando las funciones fiscalizadoras e inspectoras y los derechos de las personas que pudieran verse afectadas por ello.

Sin perjuicio de las demás normas establecidas en el presente Título, son aplicables al tratamiento de datos que efectúen los

órganos públicos, las disposiciones establecidas en los artículos 2, 14, 14 bis, 14 ter, 14 quater, 14 quinquies y 15 bis, los artículos del Párrafo Segundo y Tercero del Título II, los artículos del Título V y los artículos del Título VII de esta ley.

Artículo 22.- Comunicación o cesión de datos por un órgano público. Los órganos públicos están facultados para comunicar o ceder datos personales específicos, o todo o parte de sus bases de datos o conjuntos de datos, a otros órganos públicos, siempre que la comunicación o cesión de los datos resulte necesaria para el cumplimiento de sus funciones legales y ambos órganos actúen dentro del ámbito de sus competencias. La comunicación o cesión de los datos se debe realizar para un tratamiento específico y el órgano público receptor no los podrá utilizar para otros fines.

Asimismo, se podrá comunicar o ceder datos o bases de datos personales entre organismos públicos, cuando ellos se requieran para un tratamiento que tenga por finalidad otorgar beneficios al titular, evitar duplicidad de trámites para los ciudadanos o reiteración de requerimientos de información o documentos para los mismos titulares.

El órgano público receptor de los datos sólo puede conservarlos por el tiempo necesario para efectuar el tratamiento específico para el cual fueron requeridos, luego de lo cual deberán ser cancelados o anonimizados. Estos datos se podrán almacenar por un tiempo mayor cuando el órgano público requiera atender reclamaciones o impugnaciones, realizar actividades de control o seguimiento, o sirvan para dar garantía de las decisiones adoptadas.

Para los efectos de poder comunicar o ceder datos personales a personas o entidades privadas, los organismos públicos deberán contar con el consentimiento del titular, salvo que la comunicación o cesión de datos sea necesaria para cumplir las funciones del organismo público en materia de fiscalización o inspección.

Cuando se trate de comunicar o ceder datos personales en virtud de una solicitud de acceso a la información formulada con arreglo a lo establecido en el artículo 10 de la ley N° 20.285, los organismos públicos deberán contar con el consentimiento del titular obtenido en la oportunidad prevista en el artículo 20 de dicha ley.

Respecto de la comunicación de los datos relativos a infracciones penales, civiles, administrativas y disciplinarias, se aplicará lo dispuesto en el artículo 25 de esta ley.

Las cesiones de todo o parte de las bases de datos realizadas por un órgano público deberán constar por escrito a través

de un convenio suscrito por el cedente y el órgano o persona cesionaria de la información. En el convenio se establecerán las finalidades específicas de los tratamientos para los cuales se utilizarán los datos. La Agencia de Protección de Datos Personales en su página web pondrá a disposición de los organismos públicos modelos tipo de convenios de cesión de datos.

Los organismos públicos deberán informar mensualmente a través de su página web institucional los convenios suscritos con otros organismos públicos y con entidades privadas relativos a cesión o transferencia de datos personales. Esta obligación será fiscalizada por la Agencia de Protección de Datos Personales.

Artículo 23.- Ejercicio de los derechos del titular, procedimiento administrativo de tutela y reclamo de ilegalidad. El titular de datos podrá ejercer ante el órgano público los derechos de acceso, rectificación y oposición que le reconoce esta ley. El titular también podrá oponerse a un tratamiento específico cuando éste sea contrario a las disposiciones de este título. El titular podrá ejercer el derecho de cancelación en los casos previstos en el inciso tercero del artículo anterior.

Los organismos públicos no acogerán las solicitudes de acceso, rectificación, oposición, cancelación o bloqueo temporal de los datos personales en los siguientes casos:

a) Cuando con ello se impida o entorpezca el cumplimiento de las funciones fiscalizadoras, investigativas o sancionatorias del organismo público, y

b) Cuando con ello se afecte el deber de secreto o reserva establecido en la ley.

El ejercicio de los derechos del titular se deberá realizar de acuerdo al procedimiento establecido en el artículo 11 de esta ley, dirigiéndose al jefe superior del servicio.

El titular podrá reclamar ante la Agencia de Protección de Datos Personales cuando el organismo público le haya denegado, en forma expresa o tácita, una solicitud en que ejerce cualquiera de los derechos que le reconoce esta ley. La reclamación se sujetará a las normas previstas en el procedimiento administrativo de tutela de derechos establecido en el artículo 45 de esta ley.

Artículo 24.- Regímenes especiales. Las disposiciones de este título no se aplicarán en los siguientes casos:

a) A los tratamientos de datos personales que realicen los órganos públicos competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas las actividades de protección y prevención frente a las amenazas y riesgos contra la seguridad pública.

b) A los tratamientos de datos personales que realicen los órganos públicos competentes en materias relacionadas directamente con la seguridad de la Nación, la defensa nacional y la política exterior del país.

c) A los tratamientos de datos personales que realicen los órganos públicos competentes con el objeto exclusivo de atender una situación de emergencia o catástrofe, declarada de conformidad a la ley y sólo mientras permanezca vigente esta declaración.

Los órganos públicos y sus autoridades respectivas podrán realizar los tratamientos de datos previstos en las letras anteriores, cuando se realice para el cumplimiento de sus funciones legales, dentro del ámbito de sus competencias y de conformidad a las normas establecidas en la ley respectiva, debiendo respetar los derechos y libertades fundamentales de las personas establecidos en la Constitución Política de la República.

Con el objeto de realizar los tratamientos de datos para la finalidad prevista en la letra a) anterior, los órganos públicos y sus autoridades estarán obligadas a intercambiar información y proporcionar los datos personales que les sean requeridos para estos fines, siempre que se refieran a tratamientos que se realicen con una finalidad específica autorizada por ley o, cuando esto no sea posible, el requerimiento sea una medida necesaria y proporcional.

El ejercicio de los derechos de los titulares de datos en el marco de un proceso penal, se sujetará a las normas legales específicas que regulan el proceso penal.

Los tratamientos de datos que realicen los organismos públicos en los casos previstos en este artículo deberán cumplir con los principios de licitud del tratamiento, calidad, seguridad, responsabilidad y confidencialidad establecidos en esta ley. Asimismo, los funcionarios que participen en estos tratamientos estarán sujetos a lo dispuesto en el artículo 50.

Artículo 25.- Datos relativos a infracciones penales, civiles, administrativas y disciplinarias. Los datos personales relativos a la comisión y sanción de infracciones penales, civiles,

administrativas y disciplinarias sólo pueden ser tratados por los organismos públicos para el cumplimiento de sus funciones legales, dentro del ámbito de sus competencias y en los casos expresamente previstos en la ley.

En las comunicaciones que realicen los organismos públicos, con ocasión del tratamiento de estos datos personales, deberán velar en todo momento porque la información comunicada o hecha pública sea exacta, suficiente, actual y completa.

No podrán comunicarse o hacerse públicos los datos personales relativos a la comisión y condena de infracciones penales, civiles, administrativas o disciplinarias, una vez prescrita la acción penal, civil, administrativa o disciplinaria respectiva, o una vez que se haya cumplido o prescrito la pena o la sanción impuesta, lo que deberá ser declarado o constatado por la autoridad pública competente. Lo anterior es, sin perjuicio, de la incorporación, mantenimiento y consulta de esta información en los registros que llevan los órganos públicos por expresa disposición de la ley, en la forma y por el tiempo previsto en la ley que establece la obligación específica correspondiente. Las personas que se desempeñen en los órganos públicos están obligadas a guardar secreto respecto de esta información, la que deberá ser mantenida como información reservada.

Cuando la ley disponga que la información relativa a la comisión y sanción de infracciones penales, civiles, administrativas y disciplinarias deba hacerse pública a través de su incorporación en un registro de sanciones, o su publicación en el sitio web de un órgano público o en cualquier otro medio de comunicación o difusión, sin fijar un período de tiempo durante el cual deba permanecer disponible esta información, se seguirán las siguientes reglas:

a) Respecto de las infracciones penales, los plazos de publicidad se regirán por las normas particulares que rigen para este tipo de infracciones.

b) Respecto de las infracciones civiles, administrativas y disciplinarias, permanecerán accesibles al público por el período de cinco años.

Se prohíbe el tratamiento masivo de los datos personales contenidos en los registros electrónicos de infracciones penales, civiles, administrativas y disciplinarias que lleven los organismos públicos. El incumplimiento de esta prohibición constituye una infracción gravísima de conformidad a esta ley.

Exceptúense de la prohibición de comunicación los casos en que la información sea solicitada por los Tribunales de Justicia u otro organismo público para el cumplimiento de sus funciones legales y

dentro del ámbito de su competencia, quienes deberán mantener la debida reserva.

Artículo 26.- Reglamento. Las condiciones, modalidades e instrumentos para la comunicación o cesión de datos personales entre organismos públicos y con personas u organismos privados, se regularán a través de un reglamento expedido por el Ministerio Secretaría General de la Presidencia y suscrito por el Ministro de Hacienda, previo informe de la Agencia de Protección de Datos Personales. En este mismo reglamento se regularán los procedimientos de anonimización de los datos personales, especialmente los datos personales sensibles.

10) Reemplázase el Título V por el siguiente:

“Título V
De la transferencia internacional de datos personales

Artículo 27.- Regla general de autorización. Cumpliéndose los requisitos que de conformidad a esta ley confieren licitud al tratamiento de datos, son lícitas las operaciones de transferencia internacional de datos en los siguientes casos:

a) Cuando la transferencia se realice a una persona, entidad u organización sujeta al ordenamiento jurídico de un país que proporcione niveles adecuados de protección de datos personales.

b) Cuando la transferencia de datos quede amparada por cláusulas contractuales u otros instrumentos jurídicos suscritos entre el responsable que efectúa la transferencia y el que la recibe, y en ellas se establezcan los derechos y garantías de los titulares, las obligaciones de los responsables y los medios de control.

c) Cuando el responsable que efectúa la transferencia y el que la recibe, adopten un modelo de cumplimiento o autorregulación vinculante y certificado de acuerdo a la legislación aplicable para cada uno de ellos.

d) Cuando exista consentimiento expreso del titular de datos para realizar una transferencia internacional de datos específica y determinada.

e) Cuando se refiera a transferencias bancarias, financieras o bursátiles específicas y que se realicen conforme a las leyes que regulan estas transferencias.

f) Cuando la transferencia se efectúe entre sociedades o entidades que pertenezcan a un mismo grupo empresarial, empresas relacionadas o sujetas a un mismo controlador en los términos previstos en la Ley de Mercado de Valores, siempre que todas ellas operen bajo los mismos estándares y políticas en materia de tratamiento de datos personales. El responsable que efectúe la transferencia de datos asumirá la responsabilidad por cualquier infracción a los estándares y políticas corporativas vinculantes en que incurran algunos de los miembros del grupo empresarial. El responsable sólo podrá exonerarse de esta responsabilidad cuando acredite que la infracción no fue imputable al miembro del grupo empresarial correspondiente.

g) Cuando se deban transferir datos para dar cumplimiento a obligaciones adquiridas en tratados o convenios internacionales que hayan sido ratificados por el Estado chileno y se encuentren vigentes.

h) Cuando la transferencia resulte necesaria por aplicación de convenios de cooperación, intercambio de información o supervisión que hayan sido suscritos por órganos públicos para el cumplimiento de sus funciones y en el ejercicio de sus competencias.

i) Cuando la transferencia de datos realizada por una persona natural o jurídica, pública o privada, haya sido autorizada expresamente por la ley y para una finalidad determinada.

j) Cuando la transferencia sea efectuada con el objeto de prestar o solicitar colaboración judicial internacional.

k) Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato entre el titular y el responsable, o para la ejecución de medidas precontractuales adoptadas a solicitud del titular.

l) Cuando sea necesario adoptar medidas urgentes en materia médica o sanitaria, para la prevención o diagnóstico de enfermedades, para tratamientos médicos o para la gestión de servicios sanitarios o de salud.

Artículo 28.- Regla de determinación de países adecuados y demás normas aplicables a la transferencia internacional de datos. Se entiende que el ordenamiento jurídico de un país posee niveles adecuados de protección de datos, cuando cumple con estándares similares

o superiores a los fijados en esta ley. La Agencia de Protección de Datos Personales determinará fundadamente los países que poseen niveles adecuados de protección de datos considerando, a los menos, lo siguiente:

a) El establecimiento de principios que rigen el tratamiento de los datos personales.

b) La existencia de normas que reconozcan y garanticen los derechos de los titulares de datos y la existencia de una autoridad pública jurisdiccional o administrativa de control o tutela.

c) La imposición de obligaciones de información y seguridad a los responsables del tratamiento de los datos.

d) La determinación de responsabilidades en caso de infracciones.

La Agencia de Protección de Datos Personales pondrá en su página web a disposición de los interesados modelos tipo de cláusulas contractuales y otros instrumentos jurídicos para la transferencia internacional de datos.

Cuando no se verifique ninguna de las circunstancias señaladas en el artículo anterior, la Agencia de Protección de Datos Personales podrá autorizar, mediante resolución fundada, la transferencia internacional de datos siempre que el transmisor y el receptor de los datos otorguen las garantías adecuadas en relación con la protección de los derechos de las personas que son titulares de estos datos y la seguridad de la información transferida. La Agencia de Protección de Datos Personales podrá imponer condiciones previas para que se verifique la transferencia.

Corresponderá al responsable de datos que efectuó la transferencia internacional de datos, acreditar que ésta se practicó de conformidad a las reglas establecidas en esta ley.

Artículo 29.- Fiscalización.- La Agencia de Protección de Datos Personales fiscalizará las operaciones de transferencia internacional de datos, pudiendo formular recomendaciones, adoptar medidas conservativas y en casos calificados, suspender temporalmente el envío de los datos.”.

11) Intercálanse los siguientes Títulos VI, VII y VIII nuevos:

“Título VI
De la Agencia de Protección de Datos Personales

Artículo 30.- Agencia de Protección de Datos Personales. Créase la Agencia de Protección de Datos Personales, organismo público autónomo, descentralizado, de carácter técnico, con personalidad jurídica y patrimonio propio, sometido a la supervigilancia del Presidente de la República a través del Ministerio de Hacienda, encargado de velar por el cumplimiento de la normativa relativa al tratamiento de los datos personales y su protección. La Agencia estará afecta al Sistema de Alta Dirección Pública, sin perjuicio de las normas que se establecen en esta ley.

El domicilio de la Agencia de Protección de Datos Personales será la ciudad de Santiago.

Artículo 31.- Funciones y atribuciones. La Agencia de Protección de Datos Personales tendrá las siguientes funciones y atribuciones:

a) Aplicar e interpretar administrativamente las disposiciones legales y reglamentarias cuyo cumplimiento le corresponde vigilar, e impartir instrucciones de carácter general a las personas naturales o jurídicas que realicen tratamiento de datos personales. Las instrucciones generales que dicte deberán ser emitidas previa consulta pública efectuada a través de su página web institucional.

b) Fiscalizar y velar por el cumplimiento de los principios, derechos y obligaciones establecidos en esta ley. Para efectos de fiscalización se podrá solicitar la entrega de cualquier documento, libro o antecedente que sea necesario.

c) Resolver las solicitudes y reclamaciones que formulen los titulares en contra de los responsables de datos.

d) Investigar y determinar las infracciones en que incurran los responsables de datos y ejercer, en conformidad a la ley, la potestad sancionatoria. Para tales efectos, podrá citar a declarar, entre otros, al titular, a los representantes legales, administradores, asesores y dependientes del responsable de datos, así como a toda persona que haya tenido participación o conocimiento respecto de algún hecho que sea relevante para resolver un procedimiento sancionatorio. Asimismo, podrá tomar las declaraciones respectivas por otros medios que aseguren su fidelidad.

e) Adoptar las medidas preventivas o correctivas que disponga la ley.

f) Proponer al Presidente de la República las normas legales y reglamentarias para asegurar a las personas la debida protección de sus datos personales y perfeccionar la regulación sobre el tratamiento y uso de esta información.

g) Relacionarse con los organismos públicos y con los demás órganos del Estado, en el marco de sus funciones y competencias legales.

h) Desarrollar programas, proyectos y acciones de difusión, educación, promoción e información dirigidos a la ciudadanía y a los responsables de datos, en relación al respeto y protección del derecho a la vida privada y a la protección de los datos personales.

i) Prestar asistencia técnica, cuando le sea requerida, al Congreso Nacional, al Poder Judicial, a la Contraloría General de la República, al Ministerio Público, al Tribunal Constitucional, al Banco Central, al Servicio Electoral, a la Justicia Electoral y los demás tribunales especiales creados por ley, para la dictación y ejecución de las políticas y normas internas de estos organismos sobre el tratamiento y la protección de los datos personales.

j) Colaborar con los órganos públicos en el diseño e implementación de políticas, programas y acciones destinadas a velar por la protección de los datos personales y su correcto tratamiento.

k) Celebrar convenios o memorandos de entendimiento con organismos nacionales, internacionales o extranjeros, sean estos públicos o privados y desarrollar programas de asistencia técnica.

l) Participar, recibir cooperación y colaborar con organismos internacionales en materias propias de su competencia.

m) Asumir o solicitar al Consejo de Defensa del Estado, en conformidad a la ley, la representación judicial de sus intereses.

n) Certificar, registrar y supervisar los modelos de prevención de infracciones y los programas de cumplimiento y administrar el Registro Nacional de Cumplimiento y Sanciones.

ñ) Resolver las solicitudes o consultas relativas a si una determinada base de datos o conjunto de datos es considerada fuente de acceso público e identificar categorías genéricas que posean esta condición.

o) Ejercer las demás funciones y atribuciones que la ley le encomiende.

Artículo 32.- Coordinación regulatoria. Cuando la Agencia de Protección de Datos Personales deba dictar una instrucción general que tenga efectos en los ámbitos de competencia del Consejo para la Transparencia, de acuerdo a las funciones y atribuciones señaladas en la ley N° 20.285, le remitirá todos los antecedentes y requerirá de éste un informe para efectos de evitar o precaver conflictos de normas y asegurar la coordinación, cooperación y colaboración entre ambos órganos.

El Consejo para la Transparencia deberá evacuar el informe solicitado dentro del plazo de treinta días corridos contado desde la fecha en que hubiere recibido el requerimiento a que se refiere el inciso precedente.

La Agencia de Protección de Datos Personales valorará el contenido de la opinión del Consejo para la Transparencia expresándolo en la motivación de la instrucción que dicte, de conformidad a lo dispuesto en el artículo 41 de la ley N° 19.880. Transcurrido el plazo sin que se hubiere recibido el informe, se procederá conforme al inciso segundo del artículo 38 de esa misma ley.

A su vez, cuando el Consejo para la Transparencia deba dictar una instrucción general que tenga efectos en los ámbitos de competencia de la Agencia de Protección de Datos Personales, de acuerdo a las funciones y atribuciones señaladas en esta ley, el Consejo remitirá los antecedentes y requerirá informe a la Agencia de Protección de Datos Personales, quien deberá evacuarlo en el plazo de treinta días corridos, contado desde la fecha en que hubiere recibido el requerimiento. El Consejo valorará el contenido de la opinión de la Agencia de Protección de Datos Personales expresándolo en la motivación de la instrucción general que dicte al efecto.

Cuando la instrucción general afecte a cualquier otro órgano de la Administración del Estado, se aplicará lo dispuesto en el artículo 37 bis de la ley N° 19.880.

Artículo 33.- Del Director de la Agencia de Protección de Datos Personales. La dirección y administración superior de la Agencia de Protección de Datos Personales estará a cargo de un Director, quien será el jefe superior del Servicio.

Será designado por el Presidente de la República, conforme al Sistema de Alta Dirección Pública regulado en el título VI de la ley N° 19.882, afecto al primer nivel jerárquico, y con acuerdo del Senado adoptado por la mayoría absoluta de sus miembros en ejercicio.

El Presidente de la República deberá proponer esta designación sesenta días antes de la expiración del plazo de duración del Director saliente. El Senado dispondrá de un término de treinta días corridos para aceptar o rechazar la propuesta. En caso que no se pronuncie dentro de este plazo se entenderá aceptada la proposición del Presidente de la República. Si el Senado rechaza la proposición del Presidente de la República se deberá repetir el procedimiento hasta que se apruebe o acepte una designación. Otorgada esa aprobación o aceptación, según corresponda, el Presidente de la República, por intermedio del Ministerio de Hacienda, expedirá el decreto supremo de nombramiento del Director de la Agencia de Protección de Datos Personales.

El Director de la Agencia de Protección de Datos Personales durará cinco años en su cargo, pudiendo renovarse su nombramiento por una sola vez.

El Director cesará en sus funciones por las siguientes causales:

a) Término del período legal de su designación.

b) Renuncia voluntaria aceptada por el Presidente de la República.

c) Sobreviniencia de alguna causal de inhabilidad o incompatibilidad establecida en el artículo 34.

d) Incapacidad física o síquica para el desempeño del cargo.

e) Incumplimiento grave de sus funciones y deberes.

La remoción por las causales señaladas en las letras d) y e) será dispuesta por la Corte Suprema a requerimiento del Presidente de la República o de la Cámara de Diputados mediante acuerdo adoptado por simple mayoría. La Corte Suprema conocerá del asunto en pleno especialmente convocado al efecto y para acordar la remoción deberá reunir el voto conforme de la mayoría de sus miembros en ejercicio.

Para ser nombrado Director de la Agencia de Protección de Datos Personales, se requiere:

i. Cumplir con los requisitos generales para ingresar a la Administración Pública;

ii. Tener a lo menos siete años de ejercicio profesional;

iii. Contar con reconocido prestigio profesional o académico en el ámbito de la protección de los datos personales, y

iv. Acreditar experiencia laboral relevante en materias relacionadas con las funciones y competencias de la Agencia de Protección de Datos Personales.

Artículo 33 bis.- De las funciones y atribuciones del Director. Son funciones y atribuciones del Director las siguientes:

a) Velar por el respeto, defensa y protección del derecho a la vida privada de las personas en relación al tratamiento de sus datos personales, promoviendo una cultura de información y educación en esta materia, de acuerdo a los principios y derechos establecidos en la ley.

b) Promover la participación ciudadana en las materias relacionadas con la protección y el tratamiento de los datos personales, de acuerdo a los principios y derechos establecidos en la ley.

c) Dictar las instrucciones, circulares, oficios y resoluciones que se requieran.

d) Proponer al Presidente de la República las reformas legales o reglamentarias necesarias en el ámbito de las funciones y competencias de la Agencia de Protección de Datos Personales.

e) Interpretar administrativamente las disposiciones legales en materia de tratamiento y protección de los datos personales e impartir instrucciones para su aplicación y fiscalización.

f) Absolver las consultas sobre la aplicación e interpretación de las normas relativas al tratamiento y protección de los datos personales.

g) Planificar y dirigir las labores de fiscalización de la Agencia de Protección de Datos Personales y desarrollar políticas y programas que promuevan la prevención y la autorregulación.

h) Aplicar las sanciones de conformidad a lo establecido en esta ley y resolver los recursos legales correspondientes.

i) Dirigir, organizar, planificar y coordinar el funcionamiento de la Agencia de Protección de Datos Personales; dictar las órdenes necesarias para una marcha expedita de la misma y supervigilar el cumplimiento de las normas e instrucciones que imparta.

j) Representar a la Agencia de Protección de Datos Personales en todos los asuntos que le competan, incluidos recursos judiciales y los recursos extraordinarios que se interpongan en contra de la Dirección con motivo de actuaciones administrativas o jurisdiccionales, en coordinación con el Consejo de Defensa del Estado, según corresponda.

k) Presentar al Presidente de la República, antes del 31 de marzo de cada año, una memoria anual sobre la marcha de la Agencia de Protección de Datos Personales y dar cuenta pública de ella.

l) Resolver la celebración de los actos, contratos y convenciones necesarias para el cumplimiento de las funciones de la Agencia.

m) Delegar sus funciones y atribuciones en funcionarios de su dependencia, de conformidad a la ley.

n) Las demás funciones y atribuciones que le encomiende la ley.

Artículo 34.- Incompatibilidades e inhabilidades. El desempeño del cargo de Director exige dedicación exclusiva y es incompatible con el desempeño de todo otro cargo o servicio, sea o no remunerado, que se preste en el sector privado. Asimismo, este cargo es incompatible con todo otro empleo o servicio retribuido con fondos fiscales o municipales, y con las funciones, remuneradas o no, de consejero, director o trabajador de instituciones públicas, organismos autónomos nacionales o extranjeros, empresas del Estado y, en general, de todo servicio público creado por ley, como, asimismo, de empresas, sociedades o entidades públicas o privadas en que el Estado, sus empresas, sociedades o instituciones centralizadas o descentralizadas, tengan aportes de capital mayoritario o en igual proporción o, en las mismas condiciones, representación o participación. También es incompatible con cualquier otro servicio o empleo remunerado o gratuito en otros poderes del Estado.

El cargo de Director es compatible con el desempeño de cargos docentes en instituciones públicas o privadas reconocidas por el Estado, hasta un máximo de doce horas semanales. Del

mismo modo, el Director puede desempeñarse en organismos o asociaciones, públicas o privadas, nacionales o extranjeras, siempre que en ellas no perciba remuneración y su desempeño no sea incompatible con sus funciones.

El cónyuge o conviviente civil del Director y sus parientes hasta el segundo grado de consanguinidad inclusive, no podrán ser director ni tener participación en la propiedad de una empresa cuyo objeto o giro comercial verse sobre recolección, tratamiento o comunicación de datos personales.

No podrá ser designado Director:

1. La persona que hubiere sido condenada por delito que merezca pena aflictiva o inhabilitación perpetua para desempeñar cargos u oficios públicos, por delitos de prevaricación, cohecho y aquéllos cometidos en ejercicio de la función pública, delitos tributarios y los delitos contra la fe pública.

2. La persona que tuviere dependencia de sustancias o drogas estupefacientes o sicotrópicas ilegales, a menos que justifique su consumo por un tratamiento médico.

3. La persona que haya sido sancionada, dentro de los últimos tres años, por infracción gravísima a las normas que regulan el tratamiento de los datos personales y su protección.

En todo lo no expresamente regulado en este artículo, regirán las normas del párrafo 2° del Título III de la ley Nº 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado.

Artículo 35.- Del personal. El personal de la Agencia de Protección de Datos Personales estará afecto al decreto con fuerza de ley N° 29, de 2004, del Ministerio de Hacienda que fija el texto refundido, coordinado y sistematizado de la ley N° 18.834 sobre Estatuto Administrativo y, en materia de remuneraciones, a las normas del decreto ley N° 249, de 1974, y su legislación complementaria.

En caso que terceros ejerzan en contra del personal de la Agencia de Protección de Datos Personales, incluido su Director, acciones judiciales por actos formales o por acciones u omisiones producidas en el ejercicio de sus cargos, la Agencia de Protección de Datos Personales deberá proporcionarles defensa jurídica. Esta defensa se extenderá a todas aquellas acciones que se inicien en su contra incluso después de haber cesado en el cargo.

No procederá la defensa a que se refiere el inciso anterior en los casos en que los actos formales, acciones u omisiones en cuestión hayan configurado una causal de cesación imputable a la conducta del respectivo funcionario.

Artículo 36.- Del Patrimonio. El patrimonio de la Agencia de Protección de Datos Personales estará formado por:

a) El aporte que se contemple anualmente en la Ley de Presupuestos de la Nación.

b) Los bienes muebles e inmuebles que se le transfieran o que adquieran a cualquier título y por los frutos que de ellos se perciban.

c) Las donaciones que la Agencia de Protección de Datos Personales acepte. Las donaciones no requerirán del trámite de insinuación judicial a que se refiere el artículo 1401 del Código Civil.

d) Las herencias y legados que la Agencia de Protección de Datos Personales acepte, lo que deberá hacer siempre con beneficio de inventario. Dichas asignaciones estarán exentas de toda clase de impuestos y de todo gravamen o pago que les afecten.

e) Los aportes de la cooperación internacional.

f) Los demás aportes o recursos que se le otorguen por ley.

Título VII
De las infracciones y sus sanciones, de los procedimientos y de las responsabilidades

Artículo 37.- Régimen general de responsabilidad. El responsable de datos, sea una persona natural o jurídica, de derecho público o privado, que en sus operaciones de tratamiento de datos personales infrinja los principios, derechos y obligaciones establecidos en esta ley, será sancionado de conformidad con las normas del presente Título.

Párrafo Primero
De la responsabilidad, las infracciones y las sanciones aplicables a las personas naturales o jurídicas de derecho privado

Artículo 38.- Infracciones leves, graves y gravísimas. Las infracciones cometidas por los responsables de datos a los principios, derechos y obligaciones establecidos en esta ley se califican, atendida su gravedad, en leves, graves y gravísimas.

Las responsabilidades en que incurra una persona natural o jurídica por las infracciones establecidas en esta ley, se entienden sin perjuicio de las demás responsabilidades legales, civiles o penales, que pudieran corresponderle.

Artículo 38 bis.- Infracciones leves. Se consideran infracciones leves las siguientes:

a) Incumplimiento total o parcial del deber de información y transparencia.

b) Carecer de un domicilio o de una dirección de correo electrónico o de un medio electrónico equivalente, actualizado y operativo, a través del cual los titulares de datos puedan dirigir sus comunicaciones o ejercer sus derechos.

c) Omitir la respuesta, responder en forma incompleta o fuera de plazo, las solicitudes formuladas por el titular de datos en conformidad a esta ley.

d) Omitir el envío a la Agencia de Protección de Datos Personales las comunicaciones previstas obligatoriamente en esta ley o sus reglamentos.

e) Incumplimiento de las instrucciones generales impartidas por la Agencia de Protección de Datos Personales en los casos que no esté sancionado como infracción grave o gravísima.

f) Cometer cualquier otra infracción a los derechos y obligaciones establecidas en esta ley, que no sea calificada como una infracción grave o gravísima.

Artículo 38 ter.- Infracciones graves. Se consideran infracciones graves las siguientes:

a) Tratar los datos personales sin contar con el consentimiento del titular de datos o sin una base que otorgue licitud al

tratamiento, o tratarlos con una finalidad distinta de aquélla para la cual fueron recolectados.

b) Comunicar o ceder datos personales del titular sin su consentimiento, siendo necesario contar con aquel o cederlos para un fin distinto del autorizado.

c) Efectuar tratamiento de datos personales innecesarios en relación con los fines del tratamiento.

d) Tratar datos personales inexactos, incompletos o desactualizados en relación con los fines del tratamiento.

e) Impedir u obstaculizar el ejercicio legítimo de los derechos de acceso, rectificación, cancelación, oposición o portabilidad del titular.

f) Omitir la respuesta, responder tardíamente o denegar la petición sin causa justificada, en los casos de solicitudes fundadas de bloqueo temporal del tratamiento de datos personales de un titular.

g) Realizar tratamiento de datos personales de niños, niñas y adolescentes con infracción a las normas previstas en esta ley.

h) Realizar tratamiento de datos personales sin cumplir los requisitos establecidos para las personas jurídicas de derecho privado sin fines de lucro y cuya finalidad sea política, filosófica, religiosa, cultural, sindical o gremial, respecto de los datos de sus asociados.

i) Vulnerar el deber de secreto o confidencialidad establecido en el artículo 14 bis.

j) Vulnerar o infringir las obligaciones de seguridad en el tratamiento de los datos personales establecidas en el artículo 14 quater.

k) Omitir las comunicaciones o los registros en los casos de vulneración de las medidas de seguridad establecidas en el artículo 14.

l) Adoptar medidas de calidad y seguridad insuficientes o no idóneas para el tratamiento de datos personales con fines históricos, estadísticos o científicos y para estudios o investigaciones que atiendan fines de interés público.

m) Realizar operaciones de transferencia internacional de datos en contravención a las normas previstas en esta ley.

n) Incumplimiento de una resolución o un requerimiento específico y directo que le haya impartido la Agencia de Protección de Datos Personales.

Artículo 38 quater- Infracciones gravísimas. Se consideran infracciones gravísimas las siguientes:

a) Efectuar tratamiento de datos personales en forma fraudulenta.

b) Destinar maliciosamente los datos personales a una finalidad distinta de la consentida por el titular o prevista en la ley que autoriza su tratamiento.

c) Comunicar, transmitir o ceder, a sabiendas, información no veraz, incompleta, inexacta o desactualizada sobre el titular de datos.

d) Vulnerar el deber de secreto o confidencialidad sobre los datos personales sensibles y datos personales relativos a la comisión y sanción de infracciones penales, civiles, administrativas y disciplinarias.

e) Tratar, comunicar o ceder, a sabiendas, datos personales sensibles o datos personales de niños, niñas y adolescentes, en contravención a las normas de esta ley.

f) Omitir en forma deliberada la comunicación de las vulneraciones a las medidas de seguridad que puedan afectar la confidencialidad, disponibilidad o integridad de los datos personales.

g) Efectuar tratamiento masivo de datos personales contenidos en registros electrónicos de infracciones penales, civiles, administrativas y disciplinarias, que llevan los organismos públicos, sin contar con autorización legal para ello.

h) Realizar a sabiendas operaciones de transferencia internacional de datos en contravención a las normas previstas en esta ley.

i) Incumplimiento de una resolución de la Agencia de Protección de Datos Personales que resuelve la reclamación de un titular

sobre el ejercicio de sus derechos de acceso, rectificación, cancelación, oposición, portabilidad o bloqueo temporal.

j) Entregar información falsa, incompleta o manifiestamente errónea en el proceso de registro o certificación del modelo de prevención de infracciones.

Artículo 39.- Sanciones. Las sanciones a las infracciones en que incurran los responsables de datos serán las siguientes:

a) Las infracciones leves serán sancionadas con amonestación escrita o multa de 1 a 50 unidades tributarias mensuales.

b) Las infracciones graves serán sancionadas con multa de 51 a 500 unidades tributarias mensuales.

c) Las infracciones gravísimas serán sancionadas con multa de 501 a 5.000 unidades tributarias mensuales.

Artículo 40.- Circunstancias atenuantes y agravantes de responsabilidad. Se considerarán circunstancias atenuantes:

1) Las acciones unilaterales de reparación que realice el responsable y los acuerdos reparatorios convenidos con los titulares de datos que fueron afectados.

2) La colaboración que el infractor preste en la investigación administrativa practicada por la Agencia de Protección de Datos Personales.

3) La ausencia de sanciones previas del responsable de datos.

4) La autodenuncia ante la Agencia de Protección de Datos Personales. Junto con la autodenuncia el infractor deberá comunicar las medidas adoptadas para el cese de los hechos que originaron la infracción o las medidas de mitigación implementadas, según corresponda.

5) El haber cumplido diligentemente sus deberes de dirección y supervisión para la protección de los datos personales sujetos a tratamiento, lo que se verificará con el certificado expedido de acuerdo a lo dispuesto en el artículo 53 de esta ley.

Se considerarán circunstancias agravantes:

a) La reincidencia. Existe reincidencia cuando el responsable ha sido sancionado en dos o más ocasiones, en los últimos treinta meses, por infracción a esta ley. Las resoluciones que aplican las sanciones respectivas deberán encontrarse firme o ejecutoriadas.

b) El carácter continuado de la infracción.

c) El haber puesto en riesgo la seguridad de los titulares de los datos personales.

Artículo 41.- Determinación del monto de las multas. Para la determinación del monto de las multas señaladas en esta ley, la Agencia de Protección de Datos Personales deberá aplicar las reglas señaladas en los incisos siguientes.

La Agencia de Protección de Datos Personales deberá ponderar racionalmente cada una de las atenuantes y agravantes a fin de que se aplique al caso concreto una multa proporcional a la intensidad de la afectación.

Cuando solo concurran circunstancias atenuantes de responsabilidad, la Agencia de Protección de Datos Personales estará autorizada para aplicar al responsable, aquella sanción prevista para una infracción de menor gravedad. En los casos de las circunstancias atenuantes establecidas en las letras d) y e) del artículo anterior, la Agencia de Protección de Datos Personales podrá rebajar la sanción hasta amonestación, salvo cuando se trate de la autodenuncia de infracciones gravísimas, en cuyo caso esta rebaja sólo tendrá efecto para la primera ocasión.

En caso de que exista reincidencia, la Agencia de Protección de Datos Personales podrá aplicar una multa de hasta tres veces el monto asignado a la infracción cometida.

Efectuada la ponderación señalada en los incisos anteriores, y para establecer el monto específico de la multa, se considerarán prudencialmente los siguientes criterios:

a) Si la conducta fue realizada por el responsable con falta de diligencia o cuidado, a sabiendas o maliciosamente, en aquellos casos que no se consideran estos elementos en la configuración de la infracción.

b) Si se trata de una persona jurídica de derecho privado se deberá tener en cuenta su capacidad económica.

c) El perjuicio producido con motivo de la infracción, especialmente el número de titulares de datos que se vieron afectados.

d) Los beneficios obtenidos por el responsable a consecuencia de la infracción.

e) Si el tratamiento realizado incluye datos personales sensibles o datos personales de niños, niñas y adolescentes.

En caso de que se verifique la concurrencia de dos o más infracciones de la misma naturaleza, se aplicará la sanción correspondiente a la infracción más grave, estimándose los hechos constitutivos de una sola infracción. Si atendida la naturaleza y gravedad de las infracciones, éstas no pueden estimarse como una sola, se acumularán las sanciones correspondientes a cada una de las infracciones concurrentes.

Artículo 42.- Sanciones accesorias. En caso que se impongan multas por infracciones gravísimas reiteradas, en un período de 24 meses, la Agencia de Protección de Datos Personales podrá disponer la suspensión de las operaciones y actividades de tratamiento de datos que realiza el responsable de datos, hasta por un término de 30 días.

Durante este período el responsable deberá adoptar las medidas necesarias a objeto de adecuar sus operaciones y actividades a las exigencias dispuestas en la resolución que ordenó la suspensión.

Si el responsable no da cumplimiento a lo dispuesto en la resolución de suspensión, esta medida se podrá prorrogar indefinidamente, por períodos sucesivos de 30 días, hasta que el responsable cumpla con lo ordenado.

Cuando la suspensión afecte a una entidad sujeta a supervisión por parte de un organismo público de carácter fiscalizador, la Agencia de Protección de Datos Personales deberá previamente poner los antecedentes en conocimiento de la autoridad regulatoria correspondiente, para los efectos de cautelar los derechos de los usuarios de dicha entidad.

Artículo 43.- Registro Nacional de Cumplimiento y Sanciones. Créase el Registro Nacional de Cumplimiento y Sanciones administrado por la Agencia de Protección de Datos Personales. El registro será público y su acceso gratuito. Se consultará y llevará en forma electrónica.

En este registro se deberán consignar a los responsables de datos que hayan sido sancionados por infringir los principios y obligaciones establecidos en esta ley, la conducta infraccionada, las circunstancias atenuantes y agravantes de responsabilidad y la sanción impuesta.

Las anotaciones en el registro serán de acceso público por el período de 5 años, a contar de la fecha en que se practicó la anotación.

Artículo 44.- Prescripción. Las acciones para perseguir la responsabilidad por las infracciones previstas en esta ley prescriben en el plazo de tres años, contado desde la ocurrencia del hecho que originó la infracción.

En caso de infracciones continuadas, el plazo de prescripción de las referidas acciones se contará desde el día en que la infracción haya cesado.

Se interrumpe la prescripción con la notificación del inicio del procedimiento administrativo correspondiente.

Las sanciones que se impongan por una infracción a la presente ley prescriben en el plazo de tres años, contados desde la fecha en que la resolución que impone la sanción quede ejecutoriada.

Párrafo Segundo
De los procedimientos administrativos

Artículo 45.- Procedimiento administrativo de tutela de derechos. El titular de datos podrá reclamar ante la Agencia de Protección de Datos Personales cuando el responsable le haya denegado, en forma expresa o tácita, una solicitud en que ejerce cualquiera de los derechos que le reconoce esta ley.

La reclamación presentada se tramitará conforme a las siguientes reglas:

a) Deberá ser presentada por escrito, dentro del plazo de 15 días contado desde que reciba la respuesta negativa del responsable de datos o haya vencido el plazo que disponía el responsable para responder el requerimiento formulado por el titular. La reclamación deberá señalar la decisión impugnada, acompañar todos los antecedentes en

que se funda e indicar una dirección de correo electrónico donde se practicarán las notificaciones.

b) Recibido el reclamo, la Agencia de Protección de Datos Personales, dentro de los 10 días siguientes, deberá determinar si éste cumple con los requisitos establecidos en la letra anterior para ser acogido a tramitación. En caso de que no se acoja a trámite la reclamación, la resolución de la Agencia de Protección de Datos Personales debe ser fundada y se notificará al titular.

c) Acogido el reclamo a tramitación, la Agencia de Protección de Datos Personales notificará al responsable de datos, quien dispondrá de un plazo de 15 días para responder la reclamación, acompañando todos los antecedentes que estime pertinentes. Las notificaciones que se practiquen al responsable se realizarán a la dirección de correo electrónico a que alude la letra c) del artículo 14 ter.

d) Vencido este plazo, haya o no contestado el responsable de los datos y, sólo si existen hechos sustanciales, pertinentes y controvertidos, se podrá abrir un término probatorio de 10 días en el cual las partes pueden hacer valer todos los medios de prueba que estimen convenientes.

e) El responsable de datos en su respuesta podrá allanarse a la reclamación, en cuyo caso deberá acompañar los antecedentes o testimonios que acrediten esta circunstancia. Verificado lo anterior y notificado el titular de datos, la Agencia de Protección de Datos Personales procederá al archivo de los antecedentes, previa aplicación de la sanción, cuando correspondiere.

f) La Agencia de Protección de Datos Personales tendrá amplias facultades para solicitar antecedentes o informes que contribuyan a su resolución. Podrá convocar a las partes a una audiencia e instarlas a alcanzar un acuerdo. Las opiniones que puedan expresar los funcionarios de la Agencia de Protección de Datos Personales en esta audiencia, no los inhabilitará para seguir conociendo del asunto en caso que no se alcance un acuerdo. Logrado el acuerdo se archivarán los antecedentes.

g) La resolución del reclamo deberá dictarse por la Agencia de Protección de Datos Personales y deberá ser fundada. El procedimiento administrativo de tutela de derechos no podrá superar los seis meses.

h) La resolución de la Agencia de Protección de Datos Personales que no acoge a tramitación un reclamo y la resolución que resuelve la reclamación, podrán ser impugnadas judicialmente dentro del

plazo de 15 días contados desde su notificación, a través del procedimiento establecido en el artículo 47.

i) Junto con la interposición del reclamo, a petición fundada del titular y sólo en casos justificados, la Agencia de Protección de Datos Personales podrá suspender el tratamiento de los datos personales que conciernen al titular y que son objeto de la reclamación, debiendo previamente oír al responsable de datos.

Las reclamaciones y las solicitudes de suspensión del tratamiento formuladas en caso de rechazo de una solicitud de bloqueo temporal, deberán ser resueltas por la Agencia de Protección de Datos Personales en el más breve plazo, sin necesidad de oír previamente a las partes.

Artículo 46.- Procedimiento administrativo por infracción de ley. La determinación de las infracciones que cometan los responsables de datos por incumplimiento o vulneración de los principios, derechos y obligaciones establecidas en esta ley y la aplicación de las sanciones correspondientes, se sujetará a las siguientes reglas especiales:

a) El procedimiento sancionatorio será instruido por la Agencia de Protección de Datos Personales.

b) La Agencia de Protección de Datos Personales podrá iniciar un procedimiento sancionatorio, de oficio o a petición de parte, como resultado de un proceso de fiscalización o a consecuencia de una reclamación presentada por un titular de datos, en virtud del procedimiento establecido en los artículos 23 y 45 de esta ley. En este último caso, se deberá certificar la recepción del reclamo. Junto con la apertura del expediente, la Agencia de Protección de Datos Personales deberá designar un funcionario responsable de la instrucción del procedimiento.

c) La Agencia de Protección de Datos Personales deberá presentar una formulación de cargos en contra del responsable de datos en que describa los hechos que configuran la infracción, los principios y obligaciones incumplidos o vulnerados por el responsable, las normas legales infringidas y cualquier otro antecedente que sirva para sustentar la formulación.

d) La formulación de cargos debe notificarse al responsable de datos a la dirección de correo electrónico señalada en la letra c) del artículo 14 ter.

e) El responsable de datos tendrá un plazo de 15 días para presentar sus descargos. En esa oportunidad el responsable de

datos puede acompañar todos los antecedentes que estime pertinente para desacreditar los hechos imputados. Junto con los descargos, el responsable deberá fijar una dirección de correo electrónico a través de la cual se realizarán todas las demás comunicaciones y notificaciones.

f) Recibidos los descargos o transcurrido el plazo otorgado para ello, la Agencia de Protección de Datos Personales podrá abrir un término probatorio de 10 días en el caso que existan hechos sustanciales, pertinentes y controvertidos.

g) La Agencia de Protección de Datos Personales dará lugar a las medidas o diligencias probatorias que solicite el responsable en sus descargos, siempre que sean pertinentes y necesarias. En caso de rechazo, deberá fundar su resolución.

h) Los hechos investigados y las responsabilidades de los presuntos infractores pueden acreditarse mediante cualquier medio de prueba admisible en derecho, los que se apreciarán de acuerdo a las reglas de la sana crítica.

i) La Agencia de Protección de Datos Personales tendrá amplias facultades para solicitar antecedentes o informes que contribuyan a su resolución.

j) La resolución que ponga fin al procedimiento sancionatorio debe ser fundada y resolver todas las cuestiones planteadas en el expediente, pronunciándose sobre cada una de las alegaciones y defensas formuladas por el responsable de datos y contendrá la declaración de haberse configurado el incumplimiento o vulneración de los principios, derechos y obligaciones establecidos en la ley por el responsable o su absolución, según corresponda. En caso que la Agencia de Protección de Datos Personales considere que se ha verificado la infracción, en la misma resolución ponderará las circunstancias que agravan o atenúan la responsabilidad del infractor e impondrá la sanción, de acuerdo a la gravedad de la infracción cometida.

k) La resolución que establezca el incumplimiento o vulneración a los principios, derechos y obligaciones de esta ley y aplique la sanción correspondiente deberá ser fundada. Esta resolución debe indicar los recursos administrativos y judiciales que procedan contra ella en conformidad a esta ley, los órganos ante los que deben presentarse y los plazos para su interposición. La resolución de la Agencia de Protección de Datos Personales que resuelve el procedimiento por infracción de ley será reclamable judicialmente conforme al artículo siguiente.

l) El procedimiento administrativo de infracción de ley no podrá superar los seis meses. Cuando hayan transcurrido más de seis

meses desde la fecha de la certificación indicada en la letra b) de este artículo sin que la Agencia de Protección de Datos Personales haya resuelto la reclamación, el interesado podrá presentar un reclamo de ilegalidad en los términos previstos en el siguiente artículo.

Párrafo Tercero
Del procedimiento de reclamación judicial

Artículo 47.- Procedimiento de reclamación judicial. Las personas naturales o jurídicas agraviadas por una resolución final o de término de la Agencia de Protección de Datos Personales podrán deducir un reclamo de ilegalidad ante la Corte de Apelaciones de Santiago o la del lugar donde se encuentre domiciliado el reclamante, a elección de este último. El reclamo deberá interponerse dentro de los 15 días siguientes a la notificación de la resolución impugnada, según las siguientes reglas:

a) El reclamante señalará en su escrito, con precisión, la resolución objeto del reclamo, la o las normas legales que se suponen infringidas, la forma en que se ha producido la infracción, y cuando procediere, las razones por las cuales el acto le causa agravio.

b) La Corte podrá declarar inadmisible la reclamación si el escrito no cumple con las condiciones señaladas en la letra a) anterior. Asimismo, podrá decretar orden de no innovar cuando la ejecución del acto impugnado le produzca un daño irreparable al recurrente.

c) Recibida la reclamación, la Corte requerirá de informe a la Agencia de Protección de Datos Personales, concediéndole un plazo de diez días al efecto.

d) Evacuado el traslado o teniéndosele por evacuado en rebeldía, la Corte puede abrir un término de prueba, si así lo estima necesario, el que se regirá por las reglas de los incidentes que contempla el Código de Procedimiento Civil.

e) Vencido el término de prueba, se ordenará traer los autos en relación. La vista de esta causa gozará de preferencia para su inclusión en la tabla.

f) Si la Corte da lugar al reclamo, en su sentencia decidirá si existió agravio y ordenará, según sea procedente, la rectificación del acto impugnado y la dictación de la respectiva resolución, según corresponda.

g) Tratándose de reclamaciones en contra de una resolución que resuelve un procedimiento sancionatorio, la Corte podrá confirmar o revocar la resolución impugnada, establecer o desechar la comisión de la infracción, según corresponda y, mantener, dejar sin efecto o modificar la sanción impuesta al responsable o su absolución, según sea el caso.

h) En todo aquello no regulado por el presente artículo, regirán las normas establecidas en el Código Orgánico de Tribunales y en el Código de Procedimiento Civil, según corresponda.

Párrafo Cuarto
De la responsabilidad de los órganos públicos, de la autoridad o jefe superior del órgano y de sus funcionarios

Artículo 48.- Responsabilidad administrativa del jefe superior del órgano público. El jefe superior de un órgano público deberá velar para que el órgano respectivo realice sus operaciones y actividades de tratamiento de los datos personales con arreglo a los principios, derechos y obligaciones establecidos en el Título IV de esta ley.

Las infracciones a los principios, derechos y obligaciones en que puedan incurrir los órganos públicos se tipifican en los artículos 38 bis, 38 ter y 38 quater y serán sancionadas con multa de veinte por ciento a cincuenta por ciento de la remuneración mensual del jefe superior del órgano público infractor. La cuantía de la multa se determinará considerando la gravedad de la infracción, la naturaleza de los datos tratados y el número de titulares afectados. En la determinación de la sanción se deberán considerar también las circunstancias que atenúan la responsabilidad del infractor, especialmente la establecida en el inciso final del artículo 41.

Si el órgano público persiste en la infracción, se le aplicará al jefe superior del órgano público el duplo de la sanción originalmente impuesta y la suspensión en el cargo por un lapso de cinco días.

Tratándose de datos personales sensibles la multa será del 50% de la remuneración mensual del jefe superior del órgano público y procederá la suspensión en el cargo de hasta treinta días.

Las infracciones en que incurra un órgano público en el tratamiento de los datos personales serán determinadas por la Agencia de Protección de Datos Personales de acuerdo al procedimiento establecido en el artículo 46.

Habiéndose configurado la infracción, las sanciones administrativas señaladas en este artículo serán aplicadas por la Agencia de Protección de Datos Personales. Con todo, la Contraloría General de la República, a petición de la Agencia de Protección de Datos Personales podrá, de acuerdo a las normas de su ley orgánica, incoar los procedimientos administrativos y proponer las sanciones que correspondan.

En contra de las resoluciones de la Agencia de Protección de Datos Personales se podrá deducir el reclamo de ilegalidad establecido en el artículo 47.

Las sanciones previstas en este artículo deberán ser publicadas en el sitio web de la Agencia de Protección de Datos Personales y del respectivo órgano o servicio dentro del plazo de cinco días hábiles contado desde que la respectiva resolución quede firme.

Artículo 49.- Responsabilidad del funcionario infractor. Sin perjuicio de lo dispuesto en el artículo anterior, si en el procedimiento administrativo correspondiente se determina que existen responsabilidades individuales de uno o más funcionarios del órgano público, la Contraloría General de la República, a petición de la Agencia de Protección de Datos Personales, iniciará una investigación sumaria para determinar las responsabilidades de dichos funcionarios o lo hará en el procedimiento administrativo ya iniciado, en su caso. Las sanciones a los funcionarios infractores serán determinadas de conformidad a lo dispuesto en el Estatuto Administrativo.

En caso que el procedimiento administrativo correspondiente determine que cualquiera de los funcionarios involucrados es responsable de alguna de las infracciones gravísimas señalada en el artículo 38 quáter de esta ley, esta conducta se considerará una contravención grave a la probidad administrativa. En tales circunstancias se podrá multar a estos funcionarios por hasta el doble del beneficio pecuniario obtenido mediante la infracción. En el evento de que no sea posible determinar el beneficio económico obtenido por los infractores, se podrá aplicar una multa de hasta el 50% de la remuneración mensual del funcionario.

Artículo 50.- Deber de los funcionarios de reserva y confidencialidad. Los funcionarios de los órganos públicos que traten datos personales y especialmente, cuando se refieran a datos personales sensibles o datos relativos a la comisión y sanción de infracciones penales, civiles, administrativas y disciplinarias, deben guardar secreto o confidencialidad respecto de la información que tomen conocimiento en el ejercicio de sus

cargos y abstenerse de usar dicha información con una finalidad distinta de la que corresponda a las funciones legales del órgano público respectivo o utilizarla en beneficio propio o de terceros. Para efectos de lo dispuesto en el inciso segundo del artículo 125 del Estatuto Administrativo, se estimará que los hechos que configuren infracciones a esta disposición vulneran gravemente el principio de probidad administrativa, sin perjuicio de las demás sanciones y responsabilidades que procedan.

Cuando en cumplimiento de una obligación legal un órgano público comunica o cede a otro órgano público datos protegidos por normas de secreto o confidencialidad, el organismo público receptor y sus funcionarios, deberán tratarlos manteniendo la misma obligación de secreto o confidencialidad.

Párrafo Quinto
De la responsabilidad civil

Artículo 51.- Norma general. El responsable de datos deberá indemnizar el daño patrimonial y extrapatrimonial que cause al o los titulares, cuando en sus operaciones de tratamiento de datos infrinja los principios, derechos y obligaciones establecidos en esta ley y les cause perjuicio. Lo anterior no obsta al ejercicio de los demás derechos que concede esta ley al o los titulares de datos.

La acción indemnizatoria señalada en el inciso anterior podrá interponerse una vez ejecutoriada la resolución que resolvió favorablemente el reclamo interpuesto ante la Agencia de Protección de Datos Personales o la sentencia se encuentre firme y ejecutoriada, en caso de haber presentado un reclamo judicial, y se tramitará de conformidad a las normas del procedimiento sumario establecidas en el artículo 680 y siguientes del Código de Procedimiento Civil.

Las acciones civiles que deriven de una infracción a la presente ley prescribirán en el plazo de tres años, contados desde que se encuentre ejecutoriada la resolución administrativa o la sentencia judicial, según sea el caso, que imponga la multa respectiva.

Párrafo Sexto
Del modelo de prevención de infracciones

Artículo 52.- Artículo 52.- Modelo de prevención de infracciones. Los responsables de datos, sean personas naturales o jurídicas, públicas o privadas, deberán adoptar mecanismos para prevenir la

comisión de las infracciones establecidas en los artículos 38 bis, 38 ter y 38 quater.

Asimismo, los responsables de datos podrán voluntariamente adoptar modelos de prevención de infracciones, los que deberán contener, a los menos, los siguientes elementos:

a) Designación de un encargado de prevención o delegado de protección de datos personales.

b) Definición de medios y facultades del encargado de prevención.

El responsable de datos debe disponer que el encargado de prevención cuente con los medios y facultades suficientes para el desempeño de sus funciones, debiendo otorgarle los recursos materiales necesarios para realizar adecuadamente sus labores, en consideración al tamaño y capacidad económica de la entidad.

c) Establecimiento de un programa de cumplimiento que deberá contemplar, a lo menos, lo siguiente:

1. La identificación del tipo de información que la entidad trata, el ámbito territorial en que opera, la categoría, clase o tipos de datos o bases de datos que administra, la caracterización de los titulares de datos y el o los lugares donde residen estos últimos.

2. La identificación de las actividades o procesos de la entidad, sean habituales o esporádicos, en cuyo contexto se genere o incremente el riesgo de comisión de las infracciones señaladas en los artículos 38 bis, 38 ter y 38 quater.

3. El establecimiento de protocolos, reglas y procedimientos específicos que permitan a las personas que intervengan en las actividades o procesos indicados en la letra anterior, programar y ejecutar sus tareas o labores de una manera que prevenga la comisión de las referidas infracciones.

4. Mecanismos de reporte hacia las autoridades para el caso de contravenir lo dispuesto en la presente ley.

5. La existencia de sanciones administrativas internas, así como de procedimientos de denuncia o persecución de responsabilidades de las personas que incumplan el sistema de prevención de infracciones.

d) Supervisión y certificación del modelo de prevención de infracciones.

La regulación interna a que dé lugar la implementación del modelo y el programa, en su caso, deberán ser incorporadas expresamente como una obligación en los contratos de trabajo o de prestación de servicios de todos los trabajadores, empleados y prestadores de servicios de las entidades que actúen como responsables de datos o los terceros que efectúen el tratamiento, incluidos los máximos ejecutivos de la misma, o bien, como una obligación del reglamento interno del que trata el artículo 153 y siguientes del Código del Trabajo. En este último caso, se deben realizar las medidas de publicidad establecidas en el artículo 156 del mismo Código.

Artículo 53.- Certificación, registro, supervisión del modelo de prevención de infracciones y reglamento. La Agencia de Protección de Datos Personales será la entidad encargada de certificar que el modelo de prevención de infracciones y el programa de cumplimiento reúna los requisitos y elementos establecidos en la ley y su reglamento y supervisarlos.

La Agencia de Protección de Datos Personales creará un registro público en que consten las entidades que posean una certificación y aquellas cuya certificación haya sido revocada.

Un reglamento expedido por el Ministerio de Hacienda y suscrito por el Ministro Secretario General de la Presidencia y por el Ministro de Economía, Fomento y Turismo establecerá los requisitos, modalidades y procedimientos para la implementación, certificación, registro y supervisión de los modelos de prevención de infracciones y los programas de cumplimiento.

Artículo 54.- Atenuante especial por prevención de infracciones. Los responsables de datos que incurran en alguna de las infracciones previstas en los artículos 38 bis, 38 ter y 38 quater, podrán atenuar su responsabilidad si acreditan haber cumplido fehacientemente sus deberes de dirección y supervisión para la protección de los datos personales bajo su responsabilidad o tratamiento.

Se considera que los deberes de dirección y supervisión se han cumplido fehacientemente cuando, con anterioridad a la comisión de la infracción, los responsables de datos hubieren adoptado e implementado un modelo de organización, administración y supervisión para

prevenir infracciones, lo que deberá constar en un certificado emitido por la Agencia de Protección de Datos Personales.

Artículo 55.- Vigencia de los certificados. Los certificados expedidos por la Agencia de Protección de Datos Personales tendrán una vigencia de tres años. Sin perjuicio de lo anterior, quedarán sin efecto en los siguientes casos:

a) Por revocación efectuada por la Agencia de Protección de Datos Personales.

b) Por fallecimiento del responsable de datos en los casos de personas naturales.

c) Por disolución de la persona jurídica.

d) Por resolución judicial ejecutoriada.

e) Por cese voluntario de la actividad del responsable de datos.

El término de vigencia de un certificado por alguna de las causales señaladas precedentemente será inoponible a terceros, mientras no sea eliminado del registro.

Artículo 56.- Revocación de la certificación. La Agencia de Protección de Datos Personales puede revocar la certificación indicada en los artículos precedentes, si el responsable no da cumplimiento a lo establecido en este Párrafo. Con este objeto, la Agencia de Protección de Datos Personales podrá requerir toda aquella información que fuere necesaria para el ejercicio de sus funciones.

Los responsables pueden exceptuarse de entregar la información solicitada cuando la misma esté amparada por una obligación de secreto o confidencialidad, debiendo acreditar dicha circunstancia.

El incumplimiento en la entrega de la información requerida, así como la entrega de información falsa, incompleta o manifiestamente errónea, será sancionado en conformidad con esta ley.

Cuando un certificado ha sido revocado por la Agencia de Protección de Datos Personales, para volver a solicitarlo el responsable de datos debe acreditar fehacientemente que la causal que dio origen a su revocación ha sido subsanada.

Título VIII
Del tratamiento de datos personales por el Congreso Nacional, el Poder Judicial y organismos públicos dotados de autonomía constitucional

Artículo 57.- Regla general del tratamiento de datos personales. Es lícito el tratamiento de los datos personales que efectúan el Congreso Nacional, el Poder Judicial, la Contraloría General de la República, el Ministerio Público, el Tribunal Constitucional, el Banco Central, el Servicio Electoral y la Justicia Electoral, y los demás tribunales especiales creados por ley, cuando se realiza para el cumplimiento de sus funciones legales, dentro del ámbito de sus competencias y, de conformidad a las normas especiales que se establecen en sus respectivas leyes orgánicas y a las disposiciones del título IV de esta ley aplicables a los órganos públicos, con excepción de lo dispuesto en el artículo 14 quinquies y de lo dispuesto en el artículo 50 en lo referente a la aplicación del Estatuto Administrativo. Los funcionarios de estos organismos deberán guardar reserva de tales datos. En esas condiciones estas instituciones y organismos detentan la calidad de responsables de datos y no requieren el consentimiento del titular para efectuar el tratamiento de sus datos personales.

Corresponde a los órganos internos de las instituciones y organismos señalados en el inciso anterior ejercer las funciones y adoptar las decisiones que esta ley encomienda a la Agencia de Protección de Datos Personales.

Las autoridades superiores de los órganos internos de estas instituciones deberán dictar las políticas, normas e instrucciones necesarias para dar cumplimiento a los principios y obligaciones establecidos en esta ley, especialmente aquellas que permitan el ejercicio de los derechos que se reconocen a los titulares de datos y las que fijan los estándares o condiciones mínimas de control, seguridad y resguardo que se deben observar en el tratamiento de los datos personales, pudiendo requerir para ello la asistencia técnica de la Agencia de Protección de Datos Personales. Asimismo, las autoridades de estos órganos ejercerán la potestad disciplinaria respecto de sus funcionarios, en relación a las infracciones que se produzcan en el tratamiento de los datos personales, particularmente las infracciones señaladas en los artículos 38 bis, 38 ter y 38 quater.

Las instituciones y organismos señalados en este artículo no estarán sujetas a la regulación, fiscalización o supervigilancia de la Agencia de Protección de Datos Personales.

Artículo 58.- Ejercicio de los derechos y reclamaciones. Los titulares de datos ejercerán los derechos que le reconoce esta ley ante el Congreso Nacional, el Poder Judicial, la Contraloría General de la República, el Ministerio Público, el Tribunal Constitucional, el Banco Central, el Servicio Electoral y la Justicia Electoral, y los demás tribunales especiales creados por ley, de acuerdo a procedimientos racionales y justos, y ante los organismos que dispongan estas instituciones, de conformidad a lo señalado en el artículo anterior.

En caso que la Contraloría General de la República, el Ministerio Público, el Banco Central o el Servicio Electoral denieguen injustificada o arbitrariamente el ejercicio de un derecho reconocido por esta ley a un titular de datos, o bien infrinjan algún principio, deber u obligación establecida en ella, causándole perjuicio, el titular que se vea agraviado o afectado por la decisión del organismo, podrá reclamar ante la Corte de Apelaciones, de acuerdo al procedimiento dispuesto en el artículo 47 de esta ley.

Las autoridades superiores del Congreso Nacional, del Poder Judicial, del Tribunal Constitucional, de la Justicia Electoral y de los demás tribunales especiales creados por ley, deberán asegurarse que en el tratamiento de los datos personales que realizan estas instituciones se cumplen estrictamente con los principios y deberes y, se respeten los derechos de los titulares establecidos en esta ley, adoptando las medidas de fiscalización y control interno que resulten necesarias y adecuadas para esta finalidad.

Artículo segundo. Suprímese el literal m) del artículo 33 de la ley de Transparencia de la Función Pública y de Acceso a la Información de la Administración del Estado, contenida en el artículo primero de la ley N° 20.285.

ARTÍCULOS TRANSITORIOS

Artículo primero transitorio.- Las modificaciones a las leyes N° 19.628, sobre protección de la vida privada, y Nº 20.285, sobre acceso a la información pública, contenidas en el artículo primero y segundo, respectivamente, de la presente ley, entrarán en vigencia el día primero del mes décimo tercero posterior a la publicación de la presente ley en el Diario Oficial.

Artículo segundo transitorio.- Las bases de datos constituidas con anterioridad a la entrada en vigencia de la presente ley

deberán adecuarse a los términos previstos en ella dentro del plazo de veinte y cuatro meses, contado desde su entrada en vigencia. Con todo, los titulares de datos podrán ejercer los derechos que les confiere esta ley ante el responsable de datos, a partir de la entrada en vigencia de esta ley.

Artículo tercero transitorio.- Los reglamentos referidos en la presente ley deberán dictarse dentro de los seis meses siguientes a la entrada en vigencia de esta ley.

Artículo cuarto transitorio.- Dentro de los sesenta días anteriores a la entrada en vigencia de las modificaciones a la ley N° 19.628, sobre protección de la vida privada, contenida en el artículo primero de la presente ley, el Servicio de Registro Civil e Identificación deberá eliminar el registro de bases de datos personales contemplado en el actual artículo 22 de la ley N° 19.628.

Artículo quinto transitorio.- Facúltase al Presidente de la República para que, dentro del plazo de nueve meses contado de la fecha de publicación de esta ley, establezca mediante uno o más decretos con fuerza de ley, expedidos a través del Ministerio de Hacienda, las normas necesarias para regular las siguientes materias:

1) Fijar la planta de personal de la Agencia de Protección de Datos Personales y dictar todas las normas necesarias para la adecuada estructuración y operación de ésta. En especial, podrá determinar los grados y niveles de la Escala Única de Sueldos que se asignen a dichas plantas; el número de cargos para cada grado y planta; sus denominaciones y los niveles jerárquicos, para efectos de la aplicación de lo dispuesto en el título VI de la ley N° 19.882 y en el artículo 8 de la ley Nº 18.834, cuyo texto refundido, coordinado y sistematizado fue fijado por el decreto con fuerza de ley Nº 29, de 2004, del Ministerio de Hacienda. Asimismo, determinará las normas necesarias para la aplicación de la asignación de modernización de la ley N° 19.553 en su aplicación transitoria.

2) Determinar la dotación máxima del personal de la Agencia de Protección de Datos Personales, a cuyo respecto no regirá la limitación establecida en el inciso segundo del artículo 10 del decreto con fuerza de ley Nº 29, de 2004, del Ministerio de Hacienda.

3) Determinar la fecha de entrada en vigencia de las plantas y de iniciación de las actividades de la Agencia de Protección de Datos Personales, la que no podrá exceder de tres meses a la total tramitación del decreto con fuerza de ley que contenga la planta de personal de la Agencia de Protección de Datos Personales.

Artículo sexto transitorio.- El Presidente de la República, por decreto expedido por intermedio del Ministerio de Hacienda, conformará el primer presupuesto de la Agencia de Protección de Datos Personales, y transferirá a ella los fondos necesarios para que se cumplan sus funciones, pudiendo al efecto crear, suprimir o modificar los capítulos, asignaciones, ítem y glosas presupuestarias que sean pertinentes.

Artículo séptimo transitorio.- Dentro de los sesenta días siguientes a la publicación de la presente ley, se deberá convocar al concurso público para el nombramiento del primer director de la Agencia de Protección de Datos Personales, conforme al Sistema de Alta Dirección Pública regulado en la ley N° 19.882. El Presidente de la República podrá nombrar al director de la Agencia de Protección de Datos Personales antes de la fecha en que ésta inicie sus actividades, para efectos de la instalación de la misma. En tanto no inicie sus actividades dicha Agencia, la remuneración del Director, grado 1C, de la Escala Única de Sueldos, se financiará con cargo a la Partida del Presupuesto del Ministerio de Hacienda, Capítulo 01, Programa 01.

Artículo octavo transitorio.- Los órganos públicos que establezcan un encargado de prevención o delegado de protección de datos personales deberán designar para ello a un funcionario de la dotación vigente del respectivo organismo.

Artículo noveno transitorio.- El mayor gasto que irrogue la aplicación de esta ley en el transcurso del primer año presupuestario de vigencia será financiado con reasignaciones del presupuesto del Ministerio de Hacienda, y en lo que faltare con cargo a recursos del Tesoro Público. Para los años siguientes se estará a lo que indique la Ley de Presupuestos respectiva.”.

-.-.-

Acordado en sesiones celebradas los días 22 de marzo, 17 de abril, 17 de mayo, 29 de mayo, 19 de junio, y 5 de julio, 9 de agosto, 5 de septiembre, 3, 4, 11, 18 y 23 de octubre, 22 y 29 de noviembre, 4, 5 y 19 de diciembre, todas del año 2017, y 15, 22 y 23 de enero y 7 de marzo, todas del año 2018, con la asistencia de los Honorables Senadores señores Pedro Araya Guerrero; Alfonso De Urresti Longton (Honorable Senadora señora Isabel Allende Bussi) (Honorable Senador señor

Rabindranaht Quinteros Lara); Alberto Espina Otero (Honorable Senador señor Baldo Prokurica Prokurica), (Honorable Senador señor José García Ruminot), (Honorable Senador señor Francisco Chahuán Chahuán), (Honorable Senador señor Manuel José Ossandón Irarrázabal), (Honorable Senador señor Iván Moreira Barros); Felipe Harboe Bascuñán (Presidente) y Hernán Larraín Fernández (Honorable Senador señor Iván Moreira Barros).

Sala de la Comisión, a 14 de marzo 2018.

RODRIGO PINEDA GARFIAS
Secretario de la Comisión

RESUMEN EJECUTIVO

INFORME DE LA COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO RECAIDO EN EL PROYECTO DE LEY, EN PRIMER TRÁMITE CONSTITUCIONAL, QUE REGULA LA PROTECCIÓN Y EL TRATAMIENTO DE LOS DATOS PERSONALES Y CREA LA AGENCIA DE PROTECCIÓN DE DATOS PERSONALES. (BOLETINES Nºs 11.092-07 y 11.144 -07, refundidos)

I.- PRINCIPALES OBJETIVOS DEL PROYECTO: La iniciativa en informe tiene por objetivo perfeccionar las normas relativas al tratamiento de los datos personales de las personas naturales, de manera que éste se realice con el consentimiento del titular de dichos datos o en los casos que lo autorice la ley, asegurando estándares de calidad, información, transparencia y seguridad. Asimismo, crear la Agencia de Protección de Datos Personales, organismo público encargado de velar por la protección de los datos personales.

II.- ACUERDOS: La Comisión, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, De Urresti, Harboe y el ex Senador señor Larraín, aprobó en general esta iniciativa.

III.- ESTRUCTURA DEL PROYECTO: Se divide en dos artículos permanentes. El primero introduce diversas enmiendas a la ley N° 19.628, sobre Protección de la Vida Privada. El artículo 2° modifica la ley N° 20.285, sobre Acceso a la Información Pública. Asimismo, esta iniciativa contiene nueve disposiciones transitorias.

IV.- NORMAS DE QUÓRUM ESPECIAL: El artículo 25 y el artículo 50 tienen rango de ley de quorum calificado, en virtud de lo establecido en el inciso segundo del artículo 8° y el artículo 66 inciso tercero de la Constitución Política de la República. Los artículos 33, incisos tercero y sexto, 47, 48, inciso sexto, 49, inciso primero, 57 y 58 tienen rango orgánico constitucional toda vez que inciden en atribuciones de órganos regidos por leyes orgánicas constitucionales, y a lo dispuesto en el artículo 66 inciso segundo de la Constitución Política de la República

V.- URGENCIA: No tiene.

VI.- ORIGEN DE LA INICIATIVA: Este proyecto tiene su origen en un Mensaje de S.E la ex Presidenta de la República, señora Michelle Bachelet Jeria, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales (Boletín N° 11.144-07) y en la Moción de los Honorables Senadores señores Harboe, Araya, De Urresti, y de los ex Senadores señores Espina y Larraín, sobre protección de datos personales (Boletín N° 11.092-07).

VII.- TRÁMITE CONSTITUCIONAL: primer trámite.

VIII.- TRÁMITE REGLAMENTARIO: primer informe.

IX.- INICIO TRAMITACIÓN EN EL SENADO: **17 de enero de 2017** (Boletín N° 11.092-07) y **15 de marzo de 2017** (Boletín N° 11.144-07).

IX.- LEYES QUE SE MODIFICAN O QUE SE RELACIONAN CON LA MATERIA:

1.- Normas Constitucionales.

1.1.- El artículo 8°, inciso segundo, que establece que son públicos los actos y resoluciones de los órganos del Estado, así como sus fundamentos y los procedimientos que utilicen.

1.2 - El artículo 19 N° 4 que asegura a toda persona el respeto y protección a la vida privada y a la honra de la persona y su familia.

1.3.- El artículo 19 N° 5 que asegura a toda persona la inviolabilidad del hogar y de toda forma de comunicación privada.

1.4.- El artículo 19 N° 12 que asegura a toda persona la libertad de emitir opinión y de informar, sin censura previa, en cualquier forma y por cualquier medio.

2.- Normas legales

2.1.- Ley N°19.628, sobre protección de la vida privada.

2.2.- Ley N° 20.285, sobre acceso a la información pública.

Valparaíso, a 14 de marzo de 2018.

RODRIGO PINEDA GARFIAS
Secretario

ANEXO

INFORME DE PRODUCTIVIDAD

Proyecto de Ley que Regula la Protección y el Tratamiento de los Datos de Personales

Mensaje N°: 001-365

Ministerio de Hacienda
15.03.2017

Índice de Contenidos

I. Descripción del problema
- Ámbito de aplicación de la regulación

- Implicancias de no realizar las modificaciones regulatorias

II. Objetivos del proyecto

- Descripción de la propuesta regulatoria
- Evaluación de los objetivos
- Experiencia comparada

III. Alternativas de política consideradas

IV. Beneficios del Proyecto de Ley

1. Beneficios de la Protección de la Privacidad
2. Fomento al desarrollo de la industria de servicios globales (*Offshoring*)
3. Promoción de la industria de servicios en línea
4. Fomento a la competencia en los mercados
5. Simplificación de trámites en el Estado
6. Reducción en los costos de reclamación para los titulares de datos personales
7.

V. Posibles costos del Proyecto de Ley

1. Implementación de la Agencia de Protección de Datos Personales
2. Costos del manejo de los datos personales
3. Costos de acceso a información de actuales y potenciales clientes

VI. Conclusiones

I. Descripción del problema

La reducción en los costos de almacenamiento de la información gracias a los rápidos avances tecnológicos de las últimas décadas, ha hecho posible la obtención, el almacenamiento y el análisis de una gran cantidad de datos personales a costos cada vez más bajos. Hoy en día las empresas pueden mantener un registro detallado de todas las transacciones de sus clientes y los sitios web tienen la capacidad de almacenar información de las masivas visitas que reciben por día. Existen empresas además que recopilan datos únicos de distintas fuentes para combinarlos y elaborar perfiles detallados de los individuos, que son posteriormente vendidos a terceros para el desarrollo de nuevos negocios.

Esta realidad ha generado la necesidad de establecer las condiciones regulatorias que permitan a las personas proteger sus datos personales frente a una intromisión no consentida de terceros, sean éstos públicos o privados. En el centro de las demandas de los titulares de datos personales está el respeto a ciertos derechos, como son el derecho de acceso a su información, el derecho a rectificar datos que son inexactos, el derecho a eliminar su información en determinadas circunstancias y de oponerse al tratamiento automatizado de su información para ciertos fines. Los responsables del tratamiento de datos personales, por su parte, requieren un cuerpo legislativo coherente que establezca las condiciones bajo las cuales los datos personales pueden ser tratados de forma lícita.

Hoy la regulación sobre protección y uso de datos de carácter personal de las personas naturales está contenida en la Ley N° 19.628, del año 1999, sobre protección de la vida privada. Si bien esta ley constituyó un gran avance al momento de su publicación, siendo Chile el primer país latinoamericano en adoptar un marco regulatorio en la materia, existe amplio consenso entre los actores políticos e institucionales, organismos internacionales, académicos, entidades de la sociedad civil, empresas y la sociedad en general, que la actual normativa ha comenzado a ser insuficiente. La obsolescencia de algunos de sus criterios u orientaciones regulatorias, junto con la ausencia de una autoridad de control y de un diseño institucional adecuado la han llevado a perder eficacia en su función de protección de la privacidad de las personas en su interacción con otros y con el propio Estado.

Además, cuando Chile firmó el Convenio de Adhesión a Organización para la Cooperación y el Desarrollo Económico (OCDE) en 2010, se comprometió a seguir avanzando en las reformas de aquellas materias que son ejes para el desarrollo social y económico, tales como la protección de la privacidad y el flujo transfronterizo de datos. Dicho compromiso se cumple con el envío al Congreso de este Proyecto de Ley.

De esta forma, se propone avanzar en una nueva legislación que perfeccione y complete los vacíos de la actual normativa, equilibrando de forma adecuada la protección de los derechos y libertades de las personas que son titulares de los datos personales con el aseguramiento de la libre circulación de la información.

Ámbito de aplicación de la regulación

La regulación que se propone tendrá impacto en todas las personas naturales o jurídicas, responsables de datos, que realicen tratamiento de datos personales en Chile.

Los grupos que se ven impactados son los siguientes:

- Sector público: todos los órganos públicos que forman parte de la Administración del Estado, el Congreso Nacional, el Poder judicial, los tribunales especiales creados por ley y los órganos públicos dotados de autonomía constitucional.

- Sector privado: todos las empresas (incluyendo micro, pequeñas, medianas y grandes empresas) y las personas naturales que en el desarrollo de una actividad económica realicen el tratamiento de datos personales.

De acuerdo a información que se obtiene de la base de afiliados al Seguro de Cesantía, que maneja la Administradora de Fondos de Cesantía (AFC), existen alrededor de 332 mil empresas en el país (promedio 2016). De este total, alrededor de 260 mil son microempresas, 44 mil pequeñas empresas, 9 mil empresas medianas y sólo 3 mil son empresas de gran tamaño. Todas ellas, en mayor o menor medida, podrían verse afectadas por esta regulación.

- Sociedad civil: las ONGs, las organizaciones comunitarias, corporaciones, fundaciones y asociaciones, los partidos políticos, las asociaciones gremiales, los sindicatos, las asociaciones de consumidores, los centros de estudios, las universidades, organismos de educación y cualquier otra entidad que no desarrolle una actividad económica y que trate datos personales.

La regulación afectará también a todas las personas cuyos datos personales sean tratados en Chile, garantizándoles una serie de derechos en relación al manejo de sus datos. En la práctica, todas las personas que utilizan medios electrónicos para realizar transacciones, transitan por autopistas urbanas, emplean tarjetas de identificación o registro magnético, navegan en Internet, se registran mediante nombres de usuario y una clave en diferentes sitios web, entregan su RUT en distintos comercios para la acumulación de puntos o son parte del Registro Social de Hogares que aplica el Ministerio de Desarrollo Social, entre otras actividades, serán afectadas por la nueva regulación.

En cuanto a las actividades sujetas a la regulación, el proyecto involucra todo tratamiento de datos personales que realicen las personas naturales o jurídicas, incluidos los órganos públicos, las empresas y entidades de la sociedad civil o del tercer sector que no se encuentre regido por una ley especial. Respecto de los tratamientos de datos personales sujetos a una ley especial, se establece el carácter supletorio de esta normativa; es decir, se aplica en todos aquellos casos que no exista una regla especial.

Se encuentran excluidos de este régimen regulatorio el tratamiento de datos personales que se realice en el ejercicio de las libertades de emitir opinión y de informar regulado por las leyes especiales (ley de la Prensa) y el tratamiento de datos que efectúen las personas naturales en relación con sus actividades personales.

Implicancias de no realizar las modificaciones regulatorias

La opción política pública de mantener la actual regulación implicaría continuar con una normativa insuficiente y obsoleta, que no protege adecuadamente los derechos de la ciudadanía y que podría tener efectos económicos relevantes en la economía.

El hecho de que el país no cuente con adecuados estándares internacionales de protección de datos frena el desarrollo de las exportaciones de servicios y, en particular, el desarrollo de la industria de servicios globales. A su vez, esto impacta en la atracción de inversiones,

el desarrollo y la innovación tecnológica, y en la generación de capital humano avanzado. Asimismo, los consumidores, que pueden expresar reticencias cuando tengan la opción de utilizar servicios en línea cuando no reciben las garantías suficientes de un manejo seguro de sus datos personales, se desalienta el desarrollo de un sector emergente con gran potencial de crecimiento.

En los últimos años se han desarrollado diversas acciones para intentar subsanar, en parte, las falencias del marco normativo provisto por la Ley 19.628 de 1999 y aminorar los costos que esta situación implica. Entre estas acciones se considera un conjunto de modificaciones legales a la Ley 19.628; la utilización de modelos de autorregulación y buenas prácticas en el tratamiento y protección de los datos personales; y la judicialización de los casos de manejo ilícito de los datos personales. No obstante, ninguna de estas alternativas, en forma aislada o en su conjunto, ha sido suficiente para responder a los crecientes desafíos que esta materia involucra.

Desde su publicación, la Ley 19.628 se ha modificado en cinco ocasiones, en diversos ámbitos, con el fin de perfeccionar criterios u orientaciones regulatorias inadecuadas y completar algunos vacíos de la legislación[2]. Asimismo, están en tramitación más de 60 iniciativas legislativas, originadas mayormente en mociones parlamentarias, que han intentado regular aspectos como el tratamiento de datos personales, el tratamiento del spam, y el control del marketing directo, entre otras muchas materias. El principal problema es que estas modificaciones no han sido parte de un esfuerzo ordenado y sistemático por generar una legislación moderna que se adecúe a los estándares internacionales, como se intenta hacer en este proyecto de ley.

Por otra parte, los modelos de autorregulación asumidos por los propios responsables de datos, sin mecanismos de verificación, control y seguimiento, han sido escasos y con bajo impacto. Si bien estos mecanismos les dan mayor flexibilidad a los responsables de datos en el cumplimiento de la normativa, tienen por lo mismo una eficacia bastante limitada. Por último, la judicialización de los casos implica altos costos para los intervinientes y para el Estado y genera importantes grados de incertidumbre para los responsables de datos personales respecto a cuándo es lícito el tratamiento que realizan.

II. Objetivos del proyecto de ley

Este proyecto de ley busca avanzar en una nueva legislación que perfeccione y complete los vacíos de la actual normativa, equilibrando de forma adecuada la protección de los derechos y libertades de las personas que son titulares de los datos personales con el aseguramiento de la libre circulación de la información. Además, busca incorporar un sistema institucional y de incentivos que asegure la aplicación y cumplimiento de la ley, siempre recogiendo los estándares internacionales contenidos en la legislación comparada. En concreto, persigue los siguientes objetivos:

1. Establecer condiciones regulatorias que permitan reforzar los derechos de los titulares de los datos personales.

[2] Entre estas modificaciones se incluyen: Ley 19.812, de 2002, que introduce una serie de modificaciones para lograr una mayor reinserción laboral de aquellas personas con registros de morosidades y documentos protestados; Ley 20.285, de 2008, sobre Transparencia de la Función Pública y de Acceso a la Información de la Administración del Estado; Ley 20.463, de 2010, que suspende por un determinado plazo la información comercial de las personas cesantes. Ley 20.521, de 2011, que introduce modificaciones para garantizar que la información entregada a través de predictores de riesgo sea exacta, actualizada y veraz; Ley 20.575, de 2012, que establece el principio de finalidad en el tratamiento de datos personales.

2. Dotar al país de una normativa coherente con los estándares y compromisos internacionales, especialmente aquellos adquiridos con el ingreso de Chile a la OCDE.

3. Incrementar los estándares legales de Chile en el tratamiento de datos personales para transformarlo en un país con niveles adecuados dé protección y seguridad.

4. Definir estándares regulatorios y condiciones para legitimar el tratamiento de datos personales por parte de los órganos públicos, compatibilizando el cumplimiento de la función pública y los derechos de los ciudadanos.

5. Contar con una autoridad de control de carácter técnico y una institucionalidad pública que asuma los desafíos regulatorios y de fiscalización en materia de tratamiento de datos personales.

Descripción de la propuesta regulatoria

Para lograr los objetivos antes descritos el Proyecto de ley propone los siguientes cambios a la normativa vigente:

1. Se incorporan un conjunto de principios rectores en materia de protección y tratamiento de datos personales reconocidos en la legislación comparada.

2. Se refuerzan y amplían los derechos de los titulares de datos personales. Se le reconocen los derechos ARCO[3], derecho a la portabilidad de los datos y "derecho al olvido" en relación a los datos sobre infracciones penales, civiles, administrativas y disciplinarias.

3. Se establece un procedimiento directo y eficaz para que una persona pueda recurrir directamente ante el responsable de datos.

4. Se establece el consentimiento del titular como la principal fuente de legitimidad del tratamiento de los datos personales.

5. Se regula las obligaciones, deberes y del régimen de responsabilidades al que se sujetan las personas naturales o jurídicas que realizan tratamiento de datos personales (responsables de datos).

6. Se adoptan nuevos estándares normativos para el tratamiento de los datos personales sensibles y establecimiento de una regulación específica para cierto tipo de datos sensibles y para algunas categorías especiales de datos personales.

7. Se establece una protección y regulación especial para el tratamiento de los datos personales de niños, niñas y adolescentes.

8. Se introduce una regulación particular para el flujo transfronterizo de datos personales, que se ajusta plenamente a los estándares y recomendaciones de la OCDE.

[3] Sigla que identifica los siguientes derechos: Acceso a la información personal que está siendo tratada, Rectificación de datos inexactos o incompletos, Cancelación de datos en casos particulares y Oposición al tratamiento de su información para ciertos fines.

9. Se modernizan los estándares regulatorios para el tratamiento de datos personales por parte de organismos públicos. El tratamiento de datos personales y la cesión de los mismos será lícito sólo cuando se realice para el cumplimiento de sus funciones legales; por ejemplo, para otorgar beneficios sociales o evitar la duplicidad de trámites. Se define además un procedimiento de reclamación administrativa y de tutela judicial efectiva para el ejercicio y protección de estos derechos, y se establece que es la autoridad o jefe superior del órgano el responsable de un adecuado tratamiento de los datos personales de acuerdo a la ley.

10. Se crea una institución especializada y de carácter técnico, llamada Agenda de Protección de Datos Personales encargada de velar por el cumplimiento de la normativa relativa al tratamiento de datos personales y su protección, con facultades para regular, supervisar, fiscalizar y sancionar los incumplimientos. Se consagra un modelo de coordinación regulatoria cuando ésta deba dictar una instrucción o norma con efectos en los ámbitos de competencia del Consejo para la Transparencia.

11. Se contempla un catálogo específico de infracciones a los principios y obligaciones establecidos en la ley cometidas por los responsables de datos, que se califican atendida su gravedad. De forma coherente, se establecen sanciones que van desde la amonestación escrita a multas que oscilan entre 1 y 5.000 UTM. En casos excepcionales se contempla el cierre o clausura de las operaciones de tratamiento de datos.

Evaluación de los objetivos

El cumplimiento de los objetivos de este proyecto de ley se podrá realizar a través de distintos medios. Primero, la Agencia de Protección de Datos Personales, en virtud del ejercicio de su facultades (letras c) y d) del artículo 31), podrá requerir información a los responsables del tratamiento de datos personales y efectuar un seguimiento de la forma en que éstos ajustan sus procedimientos, a fin de dar un debido cumplimiento a la ley. Esta información permitirá realizar un análisis cualitativo de los efectos de la regulación para un manejo lícito, controlados e informado de datos personales.

Segundo, como resultado de las facultades de fiscalización y sancionatorias de la Agencia, se podrán obtener estadísticas detalladas del número y monto de las multas cursadas, el tipo de conducta constitutivo de infracción, el tamaño del perjuicio producido en términos del número de titulares afectados y los beneficios obtenidos, además del número de reclamos que formulen los titulares de datos. En conjunto con las características de los responsables de datos personales infractores (por ejemplo, tamaño, sector económico, volumen y finalidad de los datos tratados), se podrá realizar un seguimiento y un análisis cuantitativo del nivel de cumplimiento de la regulación y su efectividad distinguiendo por tipo de empresa responsable del tratamiento de datos personales. Esta información permitirá evaluar también el efecto de las sanciones como medio de disuasión.

Tercero, el proyecto de ley incorpora un modelo de prevención de infracciones, con mecanismos de verificación, control y seguimiento, al que se podrán acoger todos los responsables del tratamiento de datos personales. Dado que será la Agencia la encargada de revisar que el modelo tenga los estándares adecuados, podrá recopilar y sistematizar información relevante para la evaluación del cumplimiento de los objetivos del proyecto.

Por último, se espera que esta regulación tenga efectos económicos en el país en la medida que mejore la calidad de la normativa que resguarda el respeto a la privacidad y la protección de datos personales. Esto podría traducirse en un aumento de las exportaciones de servicios, en particular, de la industria de servicios globales, y de la

inversión en estos sectores. Asimismo, se podría observar un aumento del empleo en los sectores relevantes o que se produzca un aumento de los servicios en línea, entre otras cosas. En función de estas variables será posible realizar una evaluación de los efectos de la regulación, no sólo desde una perspectiva temporal sino también en relación a otros países.

Experiencia comparada

A nivel internacional existen dos corrientes principales en torno a la protección de los datos personales. Uno es el modelo europeo que establece como un derecho fundamental "el derecho a la protección de los datos personales"; por lo tanto, se reconoce como derecho autónomo, independiente del derecho a la privacidad. Por su parte, el modelo estadounidense enfatiza la protección de la vida privada, otorgando amplia autonomía a las personas para controlar su información, sin entorpecer la libre circulación de la misma.

Por su parte, los países miembros de la OCDE elaboraron y adoptaron las *Directrices sobre Protección de la Privacidad y Flujos Transfronterizos de Datos Personales* del organismo. Aunque no son jurídicamente vinculantes, han sido reconocidas como una declaración de los contenidos y principios esenciales que deben guiar la privacidad de los datos personales y recoger los miembros de la OCDE en sus normativas internas. Además, al establecer una estrategia común, permite evitar inconsistencias en las legislaciones internas de protección de datos personales, que podrían afectar la libre circulación de los datos y limitar los beneficios económicos del flujo transfronterizo de información.

El proyecto de ley de Protección de Datos Personales actualiza y moderniza el marco normativo e institucional incorporando a la legislación nacional un conjunto de principios rectores que han sido reconocidos en las *Directrices* de la OCDE y en los modelos regulatorios europeo y estadounidense.

Esto se traduce en que la propuesta regulatoria de esta iniciativa se establece que el tratamiento de los datos personales de las personas naturales se realice con el consentimiento del titular de estos datos o en los casos que autorice la ley, reforzando la idea que los datos personales deben estar bajo la esfera de control de su titular, como se establece en el modelo normativo estadounidense. Esto favorece su protección frente a toda intromisión de terceros y establece las condiciones regulatorias bajo las cuales los terceros, personas naturales o jurídicas, empresas u organizaciones públicas y privadas, pueden efectuar legítimamente el tratamiento de tales datos, asegurando estándares de calidad, información, transparencia y seguridad.

Además, se incorporan a la legislación interna un conjunto de principios rectores que han sido reconocidos en las *Directrices* de la OCDE y en el derecho europeo, que inspiran la regulación de las operaciones de tratamiento de datos personales: principio de licitud del tratamiento, principio de finalidad; principio de proporcionalidad; principio de calidad; principio de responsabilidad; principio de seguridad; principio de información. Además, en línea con la normativa europea, se establece una autoridad de control encargada de velar y fiscalizar el cumplimiento de la normativa relativa al tratamiento de datos personales y su protección.

De esta forma, esta regulación equilibra la protección de los derechos y libertades de las personas que son titulares de los datos personales, especialmente el respeto y protección a la vida privada e intimidad, con la libre circulación de la información, asegurando que las reglas de autorización y uso que se establezcan no entraben ni entorpezcan el tratamiento lícito de los datos por parte de los personas, organismos y empresas.

En la actualidad, todos los países miembros de la OCDE tienen una legislación sobre protección de datos personales que se alinea con las directrices de la organización, con excepción de Chile y Turquía. Así, este proyecto de ley permite cumplir un compromiso con la OCDE, adoptando las mejores prácticas internacionales y situándose a la altura de las legislaciones más avanzadas en materia de protección de la privacidad y del flujo transfronterizo de datos personales.

III. Alternativas de política consideradas

Esta propuesta regulatoria es una ley marco que actúa como regla general de aplicación, esto es, aquellos tratamientos de datos que no estén sometidos a una regla especial, se rigen por esta ley y en todo aquellos casos que estos ordenamientos particulares no regulen, se rigen supletoriamente por esta ley. Lo anterior implica que no existe duplicidad normativa o conflicto de ley, ya que esta normativa es de carácter general, pero prevalecen por sobre ella las normas especiales[4]. Respecto de la regulación aplicable al sector público, el proyecto de ley consagra dos normas de coordinación regulatoria con el objeto de evitar duplicidades, contradicciones o vacíos normativos.

En cuanto a las alternativas regulatorias para la protección de datos personales se tuvo a la vista las dos corrientes principales en la materia (modelo europeo y estadounidense, ya descritos). Reconociendo las virtudes de ambos modelos, y tomando en consideración que la Constitución Política de la República establece como un derecho fundamental de las personas el respeto y protección a su vida privada, se optó por un marco normativo que refuerza la protección de los derechos y libertades de las personas que son titulares de los datos personales, especialmente el respeto y protección a la vida privada e intimidad, pero relevando la importancia de no entorpecer la libre circulación de la información, con reglas de autorización y uso adecuadas que permitan un tratamiento lícito de los datos por parte de los personas, organismos y empresas.

Para el cumplimiento de la regulación se optó por la creación y determinación de una autoridad de control, con facultades para regular, supervisar, fiscalizar y sancionar los incumplimientos, siguiendo la orientación del modelo europeo. EE.UU., en cambio, tiene un sistema jurídico de precedentes y con amplia tutela judicial.

En este sentido, existían dos opciones institucionales: asignarle las funciones fiscalizadora, sancionadora y normativa a alguna agencia pública existente (como el Consejo para la Transparencia, CplT) o crear una nueva agencia pública.

Al respecto, la experiencia internacional indica que las facultades de vigilancia o supervigilancia en relación a la protección de datos están radicadas en la gran mayoría de
los países en agencias con responsabilidad exclusiva sobre el derecho de protección de datos. Entre estos países se pueden encontrar Australia, Austria, Bélgica, Bulgaria, Canadá, Croacia, Dinamarca, España, Finlandia, Francia, Grecia, Holanda, Irlanda, Italia, Nueva Zelandia, Portugal y Suiza. Si bien hay ejemplos de países que han adoptado la duplicidad de funciones al interior de sus instituciones, como son los casos de México y Reino Unido, las dos son experiencias muy distintas a la que se propone en Chile.

[4] Los órganos públicos que actualmente tienen normativas especiales para el tratamiento de datos personales son la Superintendencia de Pensiones para el seguro de cesantía; Ministerio de Desarrollo Social para información personal para estratificación social, aquellos encargados de la persecución penal, respecto de la investigación y sanción de delitos; el Servicio de Impuestos Internos para la fiscalización del cumplimiento tributario, entre otros.

Por otra parte, se debe considerar que los derechos de acceso a la información y de protección de datos son bienes jurídicos que por su naturaleza en muchas oportunidades pueden entrar en conflicto. Para precaver esta eventualidad, al sistema jurídico y político le corresponde generar los mecanismos para que la resolución de este conflicto tenga un cauce institucional, un procedimiento racional y competencias diferenciadas. De ahí la importancia de contar con instituciones diferentes. En un Estado de Derecho estos conflictos son resueltos, en última instancia, por los Tribunales de Justicia, pero teniendo en cuenta la opinión especializada de dos organismos diferentes (uno que pugna en favor de la transparencia en la información pública y otros que actuaría en favor de la protección de la información personal de una persona determinada). En cambio, si existiera una sola institución encargada de velar simultáneamente por la protección de datos y el acceso a la información, uno de estos dos derechos podría quedar desprotegido.

Un aspecto crítico que favorece la posición que deban existir dos instituciones distintas es que los ámbitos regulatorios de la protección de datos y del acceso a la información son muy distintos, lo que se refleja en una serie de factores:

- **Actores:** los actores sujetos a las reglas y obligaciones de acceso a la información y transparencia son principalmente entidades públicas o entidades privadas que cumplen una función pública y reciben aportes del Estado. Los actores que tratan datos personales son personas y entidades públicas o privadas.

- **Principios:** Los principios que orientan a las instituciones que regulan estas actividades tienen orígenes y focos distintos, incluso pueden ser contradictorios. El acceso a la información tiene como principios centrales de actuación la transparencia y el acceso a la información pública. En tanto que la protección de datos se centra en el consentimiento de la persona o titular (tratamiento controlado) y en el uso de la información (principios de licitud y finalidad del tratamiento).

- **Funciones y regulaciones:** El ámbito regulatorio de la protección de datos está orientado hacia la generación de estándares normativos que favorezcan un tratamiento de datos controlado, seguro y con amplios grados de autonomía personal para los titulares de datos. En el acceso a la información el foco de la regulación está en el ejercicio de la función pública con transparencia, promoviendo el conocimiento de los procedimientos, contenidos y decisiones que se adopten en su ejercicio.

- **Especialización:** Las regulaciones en el ámbito del acceso a la información y la transparencia exigen un alto nivel de conocimiento técnico en los modelos de toma de decisiones, procesos y actividades de los órganos de la Administración del Estado. Las regulaciones relativas a la protección de datos exige altos niveles de conocimiento en los mercados de la información personal, el intercambio de datos y la interacción con las nuevas tecnologías de la información *(big data,* internet de las cosas, dispositivos móviles inteligentes, entre otros).

- **Conflictos de intereses:** La institucionalidad ligada a acceso a la información está pensada principalmente en su independencia frente al Poder Ejecutivo. En el caso de la protección de datos los principales conflictos de intereses se darán con el sector

privado, por ende el problema se torna mucho más complejo.

En consideración a los planteamientos antes presentados, el Ejecutivo en este proyecto de ley optó por un modelo de autoridad basado en el control especializado y con altos estándares técnicos, que le otorga a la Agencia de Protección de Datos Personales una única función de protección de datos personales.

IV. Beneficios del proyecto de ley

El principal objetivo de este proyecto de ley es salvaguardar el respeto y la protección de los derechos y las libertades de las personas; en particular, el derecho a la privacidad frente a una intromisión no consentida de terceros, sean estos públicos o privados y, regular el tratamiento ilícito de la información de los titulares de datos.

La literatura reconoce un conjunto de *trade-offs* económicos asociados a la difusión y protección de datos personales. Sin embargo, no todos estos *trade-off* tienen una dimensión monetaria explícita. En particular, la protección de la privacidad incide en el bienestar de las personas de manera no sólo intangible, sino que muchas veces no medible. Más allá de esto, se puede distinguir una serie de beneficios económicos que se desprenden de avanzar en una nueva legislación que garantice un adecuado tratamiento de los datos personales.

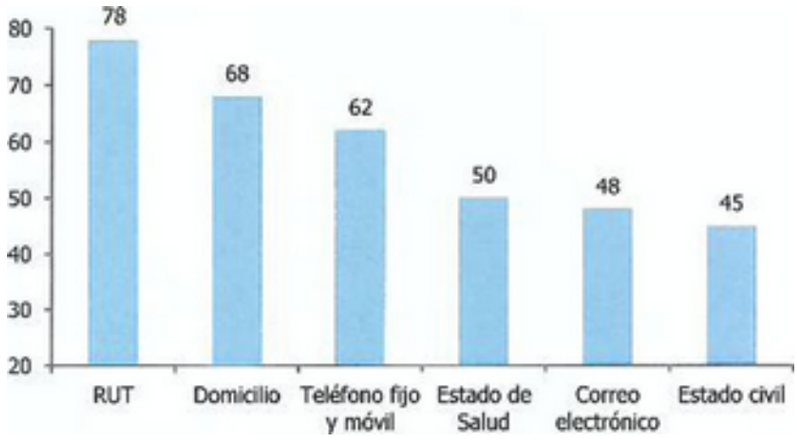
Los beneficios más relevantes a destacar y que son analizados en este informe son los siguientes:

1. Beneficios de la Protección de la Privacidad

Uno de los principales beneficios del proyecto de ley dice relación con el efecto en bienestar que se deriva de la mayor protección de la privacidad. Estudios de opinión realizados en distintos países muestran que los consumidores tienen una preocupación especial por la privacidad de su información personal[5]. Un estudio del Consejo para la Transparencia (CPLT), muestra que las personas se preocupan del cuidado de su información personal, especialmente cuando se refiere a su RUT, domicilio, y teléfono fijo y móvil (Gráfico 1).

Gráfico 1: Porcentaje de las personas que cuida distintos tipos de información personal, 2014

[5] En 2000, un estudio de la Comisión Federal del Comercio (FTC, por sus siglas en inglés) reportó que 67% de los consumidores estaban "muy preocupados" por la privacidad de la información personal que entregan en línea. En 2005, en una encuesta de la cadena de noticias CBS en EE.UU., la mayoría de los estadounidenses declaró que su privacidad estaba "en peligro". Asimismo, en 2009, una encuesta de Turow et al. (2009) mostró que la mayoría de los estadounidenses se resisten a recibir publicidad "a la medida".



Fuente: Protección do Datos Personales en el Manejo de Datos de Investigación realizado Organismos Públicos, Unidad de Estudios y Publicaciones, Dirección de Estudios, Consejo para la Transparencia, 2015.

Una valoración económica experimental de los datos personales se realizó para el caso mexicano. Una persona valora en hasta US$ 253 la información altamente sensible -RUT e información bancaria- mientras su valoración cae hasta US$ 6 cuando se trata simplemente de su información básica. Utilizando información contenida en pólizas de seguros para proteger a las personas contra el robo de su identidad, u otras herramientas se puede obtener otra aproximación de la valorización que dan las personas a su información personal. Así, por ejemplo, en México, las pólizas para proteger el robo de la identidad se transan en US$ 168, a su vez, las herramientas para eliminar registros cuestan US$ 152 y un *software* de navegación para proteger la identidad vale US$ 108[6].

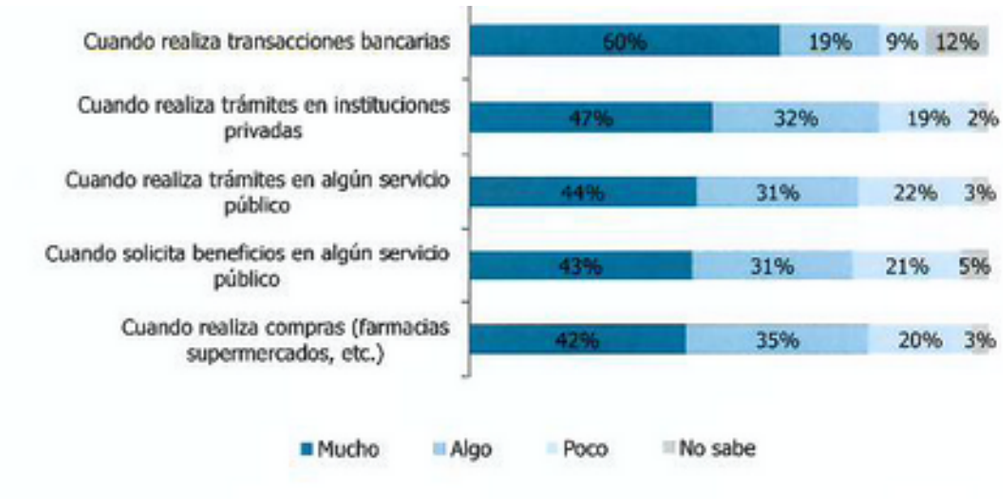
Una encuesta realizada en México, con una metodología precisa para medir la disposición a pagar por la protección de los datos personales y lo que se estaría dispuesto a aceptar (recibir) por la venta de los propios datos personales, muestra que estos están en torno a US$ 656 y US$ 1.525, respectivamente. Es interesante notar que las personas estarían dispuestas a aceptar por la venta de sus datos personales 2,3 veces más que lo que estarían dispuestos a pagar por la protección de los mismos.

El costo del mal uso de la información personal -y por ende, el beneficio de protegerla—es complejo de medir en la medida que involucra daños tanto tangibles como intangibles, que incluso pueden llegar a manifestarse tiempo después. Calo (2011) distingue entre daños objetivos y subjetivos a la privacidad[7]. Los primeros se vinculan a la pérdida de control de la información personal y a la posibilidad de usar los datos de una persona en contra de ella (por ejemplo, el uso malicioso del RUT de una persona). El estudio del CPLT ya citado muestra que cuando las personas más se preocupan por el mal uso de su información personal es en las transacciones bancadas y en trámites con instituciones privadas (empresas de servicios, grandes tiendas, etc.) (Gráfico 2). Los daños subjetivos se derivan de la percepción de observación indeseada, que pueden generar ansiedad, incertidumbre e incluso temor.

Gráfico 2: Situaciones en las cuales las personas se preocupan de su información personal, 2014

[6] AMIPQ (2014). Estudio sobre el Valor Económico de los Datos Personales.

[7] Calo, R. (2011). The boundaries of privacy harm. Indiana Law Journal 86.



Fuente: Protección de Datos Personales en el Manejo de Datos de Investigación realizado Organismos Públicos, Unidad de Estudios y Publicaciones, Dirección de Estudios, Consejo para la Transparencia, 2015.

La existencia de mercados secundarios de datos de consumidores también puede producirles externalidades negativas. Esto, ya sea porque la empresa responsable de los datos extrae todo el beneficio de la información de los consumidores para fines comerciales o publicitarios, o porque obtiene todas la ganancias de transferir la información a terceros, pero sin internalizar los costos para los consumidores de relevar esta información. Dado que los consumidores no tienen cómo saber quién divulga su información o incluso cómo es cruzada con otras fuentes de datos, no son capaces de penalizar adecuadamente a la empresa que ilícitamente hizo uso de su información (Swire y Litan, 1998[8]). En términos económicos, la empresa internaliza las ganancias de usar la información de sus consumidores, pero externaliza varios de los costos.

Por la naturaleza incierta del costo de la privacidad, las personas tienen muchas dificultades para poder cualificarlos y evaluarlos adecuadamente. No obstante, esto no significa que no existan; pueden ser eventos con alta probabilidad y bajo impacto para las personas (por ejemplo, el *spam)* o materializarse como eventos con un impacto alto pero con baja ocurrencia probabilistica (por ejemplo, rechazo de un crédito hipotecario por suplantación de identidad). En cualquier caso, ya sea por su bajo impacto o escasa probabilidad de ocurrencia, pueden ser ignorados a nivel individual, aunque en el agregado podrían causar un daño social significativo.

[8] *Swire, P. P. y R. E. Litan (1998). None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive. Washington, DC: Brookings Institution Press.*

2. Fomento al desarrollo de la industria de servicios globales *(Offshoring)*[9]

En la actualidad a las empresas extranjeras de servicios globales se les dificulta instalarse en Chile, porque el país no cuenta con adecuados niveles de protección de datos y las empresas no tienen garantías suficientes de un manejo lícito de la información privada tratada dentro del país. Para poder operar hoy en Chile, las empresas de servicios globales solicitan una autorización para tratar datos personales al regulador extranjero del país correspondiente, lo que encarece el proceso y disminuye las ventajas comparativas de Chile para competir en los mercados internacionales. Así, muchas empresas de servicios evalúan el país donde se instalan dependiendo de si cumple o no los estándares en materia de protección de datos establecidos por la OCDE.

Pese a todo, Chile ha tenido un buen desempeño en el desarrollo de la industria de servicios globales y existe un gran potencial para continuar impulsándolo. No sólo porque el *offshore* de servicios es una industria en rápido crecimiento, que casi cuadruplicó su tamaño entre los años 2005 y 2010[10], sino también porque Chile tiene importantes ventajas comparativas en términos de costos, habilidades y clima de negocios. Es uno de los países de la región más avanzados en materia de conexión digital, uso de TIC y capital humano, además de que comparte huso horario con EE.UU, factores todos que son clave para el desarrollo del sector de exportaciones de servicios. De hecho, el 2008 (último año con información disponible), la industria de servicios globales en Chile exportó US$ 843 millones, aportando a la generación de 20.034 puestos de trabajo.

La disminución en las barreras a los flujos transfronterizos de datos, como resultado de la adaptación de la normativa vigente a los estándares internacionales, y su consiguiente impacto positivo en la industria de servicios globales, podría contribuir de manera indirecta a aumentar el empleo y el capital humano calificado. Al mismo tiempo, al incentivar la transferencia de tecnología y diversificar la oferta exportable, reduciría la vulnerabilidad de la economía chilena a los vaivenes de la economía mundial.

3. Promoción de la industria de servicios en línea

El reforzamiento de los derechos de los titulares de datos personales, ya sea a través de un mayor control de la información que los consumidores entregan o una disminución de las vulneraciones a las medidas de seguridad, podría impactar positivamente en el desarrollo de la industria de servicios en línea.

Las vulneraciones a las medidas de seguridad; que ocasionan la destrucción; filtración; pérdida o alteración de sus datos personales o un acceso no autorizado a ellos, tienen costos relevantes para las personas. Esto es, desde los costos económicos que implican operaciones fraudulentas por compras en línea, o el hecho que la simple incertidumbre que genera saber que una empresa no está protegiendo adecuadamente la información puede llevar a no usar un servicio o comprar un producto. De la misma manera, diversos estudios muestran que en la medida que los consumidores tienen mayor control sobre la

[9] El *Offshoring* es un modelo de negocios en que las empresas trasladan actividades y/o procesos al exterior, ya sea mediante la constitución de una subsidiaria en el exterior (inversión extranjera directa) o mediante la subcontratación de un tercero extranjero (exportación de servidos). Los servidos globales incluyen una amplia variedad de actividades, que pueden subdividirse en: i) procesos de tecnología de la información, ii) procesos de negocios y iii) procesos de conocimiento, así como actividades verticales específicas por industria. Las empresas realizan operaciones de *offshoring* para reducir costos, así como para mejorar la calidad y diversificar costos.

[10] El mercado global de offshoring pasó de US$ 57,1 billones en 2005 a US$ 201,9 billones en 2010.

información que relevan en las redes sociales, por ejemplo, porque pueden ejercer sus derechos ARCO, sienten mayor confianza y tranquilidad para continuar entregando información de ellos mismos.

4. Fomento a la competencia en los mercados por la portabilidad

El derecho a la portabilidad de los datos incentiva la competencia y el desarrollo de nuevos productos, en la medida que obliga a las empresas a entregar toda la información que ellos manejan respecto a un titular de datos personales. Por ejemplo, en el mercado de la telefonía móvil si los consumidores no pueden medir con exactitud cuánto utilizan su teléfono móvil podrían permanecer en un plan, que no es adecuado de acuerdo a su consumo, siendo que buscando en otras compañías podrían encontrar una alternativa que les entregue el mismo servicios a un precio más bajo. Con esta información, los consumidores fuerzan a las empresas a competir por ofrecerles un mejor precio, lo que a su vez se traduce en un aumento en la competencia y en el desarrollo de nuevos productos, así como en el surgimiento de empresas intermediarias que podrían facilitar la búsqueda de mejores tarifas para los consumidores. Precisamente en el caso de las compañías de teléfonos celulares, los consumidores en el Reino Unido perdieron US$ 7,35 billones en 2011 por quedarse en la compañía equivocada.

5. Simplificación de trámites en el Estado

El proyecto de ley regula con precisión la facultad de los órganos públicos para comunicar o ceder datos personales específicos o bases de datos entre organismos públicos, cuando ellos se requieran para un tratamiento que tenga por finalidad otorgar beneficios al titular, evitar duplicidad de trámites para los ciudadanos o reiteración de requerimientos de información o documentos para los mismos titulares.

6. Reducción en los costos de reclamación para los titulares de datos personales

En los procedimientos administrativos (de tutela de derecho y de infracción de ley) que se establecen en este proyecto de ley (artículos 45 y 46), los titulares de datos personales no deberán incurrir en costos que sí tienen lugar en la ley vigente, tales como la contratación de abogados para presentar recursos ante el juzgado de letras en lo civil y el costeo de trámites tales como las notificaciones judiciales. El titular de datos que se vea afectado en sus derechos da inicio al procedimiento a través de la presentación de una reclamación ante la Agencia de Protección de Datos Personales, proceso que puede realizarse completamente en línea. Esta reducción en los costos de transacción también favorecerá a los responsables de datos personales.

V. Posibles costos del Proyecto de Ley

El principal costo directo de la propuesta regulatoria contenida en este proyecto de ley es la implementación y el funcionamiento de la Agencia de Protección de Datos Personales. Pero existe también otra serie de posibles costos derivados de un cambio en los procedimientos para manejar los datos personales por parte de los responsables, y de un acceso algo más difícil a la información de los consumidores por parte de las empresas.

Para minimizar estos posibles costos, en el proyecto de ley se establece una gradualidad en la implementación de la regulación y se establece un modelo de prevención de

infracciones, a cargo de la Agencia de Protección de Datos. La adopción de modelos de cumplimiento implica, en el mediano plazo, importantes ahorros en los costos administrativos, reducción de contingencias y la generación de una cultura institucional que previene y anticipa riesgos, además de promover el cumplimiento de la ley.

Los costos más relevantes a destacar y que son analizados en este informe son los siguientes:

1. Implementación de la Agencia de Protección de Datos Personales

La propuesta de creación de la Agencia de Protección de Datos Personales tendrá un mayor gasto fiscal en régimen de $ 1.428.876 miles, a partir del segundo año de vigencia de la ley. Respecto a la distribución de estos gastos, el Cuadro 1 presenta el desglose para año 1 y años siguientes en régimen.

Cuadro 1: Distribución de gastos

(miles de pesos de 2017)

Remuneraciones	711.401	1.166.196
Gasto corriente	169.057	262.680
Inversión inicial	417.560	-
Total Gastos	**1.298.018**	**1.428.876**

Fuente: Informe Financiero N° 021 - 15/03/2017.

Tal como señala el informe financiero del proyecto de ley, la Agencia de Protección de Datos Personales, contará con una Dirección Nacional, 3 Divisiones (Fiscalización y Promoción, Regulación y Jurídica), además de un Departamento de Administración, con 21 funcionarios ingresando el primer año y 33 a partir del segundo (Cuadro 2). Asimismo, se requerirá una inversión inicial para la adquisición de equipamiento de oficinas e informática, así como habilitación de oficinas.

Cuadro 2: Estructural del personal y costos

(miles de pesos de 2017)

Director Nacional	1	1C	7.773	93.281
Jefes de División	4	3	20.464	245.567
Jefes de Departamento	1	4	4.610	55.324
Jefes de Subdepartamento	2	5	7.198	86.370
Profesionales	20	4°-9°	53.762	645.140
Secretarias	3	12°-20°	2.202	26.421
Chofer	1	18	693	8.321
Auxiliar	1	24	481	5.772
Total		**33**	**97.183**	**1.166.196**

Fuente: Informe Financiero N° 021 - 15/03/2017.

2 Costos del manejo de los datos personales

La regulación propuesta podría generar un aumento en los costos administrativos de los responsables de datos para cumplir con la regulación. Estos costos podrían clasificarse en 3 tipos:

a. **Gestión de los datos:** Los responsables deberán mejorar la gestión de los datos personales implementando mecanismos y herramientas tecnológicas que permitan que el titular ejerza sus derechos en forma expedita, ágil y eficaz; deberán reportar a la Agencia las vulneraciones a las medidas de seguridad; deberán mantener permanentemente a disposición del público una serie de datos respecto a los datos que manejan y su política de tratamiento de datos personales.

b. **Atención de reclamos:** El proyecto establece plazos bien definidos y acotados para que los responsables de datos respondan a los requerimientos de los titulares de datos.

c. **Medidas de prevención y servicios de** *compliance.* El proyecto genera incentivos para que los responsables inviertan en detectar el tratamiento de datos riesgosos, mejorar la trazabilidad de los procesos y determinar mecanismos adecuados para detectar filtraciones de datos. Durante los primeros meses de adaptación a la nueva regulación, los responsables de datos podrían encontrar óptimo contratar empresas de *compliance*[11].

3. Costos de acceso a información de actuales y potenciales dientes

El eventual aumento en los costos de acceder a la información de potenciales clientes podría generar problemas de riesgo moral y selección adversa en algunos mercados donde existen asimetrías de información[12]. Asimismo, podría encarecer el costo de obtener

[11] Un análisis cualitativo en Hoofnagle (2007) da cuenta de que las empresas en EE.UU. aumentan sus gastos administrativos y en seguridad luego de la publicación de varias leyes que penalizan las filtraciones de datos.

[12] Se produce riesgo moral cuando un individuo toma más riesgo porque sabe que son otras personas las que soportan las consecuencias de los mayores riesgos asumidos. En cambio, se produce selección adversa, previo a la firma de un contrato, cuando la parte menos informada no es capaz de distinguir la buena o mala

información no sólo para las empresas que actualmente operan (incumbentes), sino también para las potenciales entrantes. Como éstas no conocen el mercado, podrían tener mayores dificultades para acceder a sus potenciales clientes, generándose un eventual aumento de las barreras a la entrada, disminuyendo la competencia en favor de las empresas con grandes bases de datos de clientes en dicho mercado y provocando una mayor concentración de los mercados.

Los consumidores se benefician directamente cuando las empresas pueden acceder a flujos relevantes de información respecto a sus preferencias y comportamiento. Las empresas pueden ofrecer a sus clientes recomendaciones personalizadas, que son más útiles para ellos, en base a su comportamiento observado (compras, búsquedas, visitas, clicks en una página web); dirigir más efectivamente su publicidad reduciendo la cantidad de información irrelevante para los clientes o incluso puede entregarles directamente cupones de descuento; y mejorar sus servicios o rediseñarlos para adecuarlos a las necesidades de sus clientes. En este sentido, la limitación del flujo de información podría traducirse en una pérdida de opciones que podrían ser interesantes para los consumidores.

VI. Conclusiones

El acelerado desarrollo tecnológico, la masticación en el uso de las tecnologías de la información, el extendido acceso a internet, la generación y uso de grandes volúmenes de información a través de sistemas automatizados de procesamiento, la expansión del comercio electrónico, sumado a los nuevos desafíos que enfrentan las sociedades en materia de reconocimiento y protección de los derechos de las personas, hacen necesario avanzar en una nueva legislación que perfeccione y complete los vacíos de la actual normativa.

Además, se hace necesario el cumplimiento del compromiso de Chile, adquirido con la OCDE con la firma del Convenio de Adhesión, respecto a seguir avanzando en las reformas de aquellas materias que son ejes para el desarrollo social y económico, tales como la protección de la privacidad y el flujo transfronterizo de datos.

Uno de los principales beneficios del proyecto de ley dice relación con el efecto en bienestar que se deriva de la mayor protección de los derechos y las libertades de las personas, en particular el derecho a la privacidad frente a una intromisión no consentida de terceros, sean estos públicos o privados. Las personas tienen una preocupación especial por la privacidad de su información personal y están dispuestas a desembolsar sumas relevantes de recursos para protegerse frente al mal uso de ésta. Sin embargo, se debe considerar que la protección de la privacidad incide en el bienestar de las personas de manera no sólo intangible, sino que muchas veces no medible, por lo que es complejo estimar su potencial impacto en la economía.

Se puede distinguir una serie de beneficios económicos que se desprenden de avanzar en una nueva legislación que garantice un adecuado tratamiento de los datos personales. Entre ellos, destaca el fomento al desarrollo de la industria de servicios globales, que tiene un tremendo potencial de crecimiento, además de contribuir a generar más empleo y aumentar la demanda por capital humano calificado. Esto también puede contribuir a incentivar la transferencia de tecnología y diversificar la oferta exportable, reduciendo la vulnerabilidad de la economía chilena a los vaivenes de la economía mundial.

calidad de lo ofrecido por la otra parte.

Asimismo, el reforzamiento de los derechos de los titulares de datos personales tendrá un impacto en el desarrollo de servicios en línea, y fomentará la competencia en los mercados por la portabilidad de los datos personales. Para éstos también implicará una disminución en los tiempos que dedican a hacer trámites frente al Estado, porque se termina con la duplicidad de trámites o la reiteración de requerimientos de información, en la medida que se establece un procedimiento claro para que los órganos públicos puedan comunicar o cederse información de forma lícita entre ellos. Otra ventaja para los consumidores es que en caso que una persona sienta que sus derechos han sido vulnerados, puede dar inicio a un procedimiento a través de la presentación de una reclamación ante la Agencia de Protección de Datos Personales, en forma completamente en línea y gratuita. Con la ley vigente, las personas deben incurrir en costos de contratación de abogados para presentar recursos ante el juzgado de letras en lo civil y de trámites tales como las notificaciones judiciales.

En cuanto a los costos de esta regulación, estos se derivan de la implementación y funcionamiento de la Agencia de Protección de Datos Personales y del cambio en los procedimientos para manejar los datos personales por parte de los responsables. Esto podría hacer más difícil el acceso a la información relevante de los consumidores por parte de las empresas; sin embargo, se establece una gradualidad en la implementación de la regulación y un modelo de prevención de infracciones, a cargo de la Agencia de Protección de Datos, para minimizar estos costos.

El modelo regulatorio que se presenta equilibra de forma adecuada la protección de los derechos y libertades de las personas que son titulares de los datos personales, sin entrabar ni entorpecer la libre circulación de la información, para no limitar los beneficios económico del flujo de información.

En suma, los beneficios que trae el cambio regulatorio que contiene este proyecto de ley superan ampliamente los posibles costos asociados a esta propuesta. En este sentido, se justifica plenamente avanzar en esta nueva legislación que perfeccione y complete los vacíos de la actual normativa, y ponga a Chile a la altura de los países más avanzadas en la protección de su información personal.

REPUBLICA DE CHILE
MINISTRO
MINISTERIO DE HACIENDA

RODRIGO VALDÉS PULIDO
Ministro de Hacienda

ÍNDICE

Página

1.- Normas de quorum especial 4

2.- Constancia reglamentaria 5

3.- Antecedentes 6

a) De Derecho 6

b) De Hecho	6
4.- Discusión en general	44
5.- Aprobación de idea de legislar	206
6.- Discusión en particular	206
7.- Texto del proyecto	578
8.- Resumen Ejecutivo	640
9.- Anexo	642