Observaciones y Propuestas del Consejo para la Transparencia

Proyecto de Ley sobre Protección de Datos Personales (Boletín N° 11.092-07) y Proyecto de Ley 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)

DJ/UNR/15.05.2017

En ejercicio de la facultad de proponer al Presidente de la República y al Congreso Nacional perfeccionamientos normativos para asegurar la transparencia y el acceso a la información (artículo 33, letra f), de la Ley de Transparencia), mediante el presente documento el Consejo para la Transparencia da a conocer sus observaciones y propuestas, respecto del "Proyecto de Ley sobre Protección de Datos Personales (Boletín N° 11.092-07, en adelante "Moción") y del "Proyecto de Ley 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 adelante "Proyecto del Ejecutivo"), ambos actualmente en primer trámite constitucional ante la Comisión de Constitución, Legislación, Justicia y Reglamento del Senado.

El presente documento hace propuestas y sugerencias en diez materias de la reforma a la legislación de datos personales. Cada propuesta es detallada y explicada en relación a la Ley 19.628, la Moción y el Proyecto del Ejecutivo. Las materias abordadas son las siguientes:

1. Objeto de la ley y ámbito de aplicación.
2. Definiciones y principios.
3. Consentimiento, datos sensibles y datos especialmente protegidos.
4. Derechos ARCO.
5. Responsable y encargado.
6. Regulación de las competencias de los órganos del Estado.
7. Transferencia internacional de datos personales.
8. Autoridad de control.
9. Infracciones y sanciones.
10. Entrada en vigencia y autorregulación.

1. Objeto y ámbito de aplicación de la ley

a. Objeto de la ley. Uno de los aspectos fundamentales en un cuerpo normativo que aspira a regular de manera integral el tratamiento de datos personales, está dado por su objeto y ámbito de aplicación.

En lo que respecta a la finalidad de la ley, el mensaje del Ejecutivo 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. Por otro lado, la moción de los senadores propone como 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.

Es conveniente ajustar el objeto del proyecto de ley a la protección de datos personales, entendiendo que el derecho a la autodeterminación informativa es distinto del derecho de respeto y protección a la vida privada. En efecto, se encuentra actualmente en la Cámara de Diputados, en su segundo trámite constitucional, un proyecto de ley (Boletín Nº 9384-07) que busca reconocer explícitamente este derecho en nuestro ordenamiento jurídico, consagrándolo constitucionalmente[1]. En base a lo anterior, se sugiere optar por la redacción de la Moción por dos razones. Primero, porque está alineada con la autodeterminación informativa como derecho fundamental, entendida ésta como la "*facultad del individuo de decidir por sí mismo, cuando dentro y de qué límites procede revelar situaciones referentes a la vida privada*"[2]. Segundo, porque separa conceptualmente la protección de datos personales del derecho de respeto y protección a la vida privada.

Propuesta de objeto de la ley
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.*

[1] Boletín Nº 9384-07, Proyecto de Ley iniciado en moción, que consagra el derecho a protección de los datos personales.
[2] Sentencia del Tribunal Constitucional Federal Alemán, del 15 de Diciembre de 1983, Boletín de Jurisprudencia Constitucional Nº 33, pag. 126, traducción Mariano Daranas.

b. Ámbito de aplicación. Crecientemente, el tratamiento de datos personales se efectúa transnacionalmente. En efecto, los datos son almacenados y compartimentalizados en distintos servidores, especialmente, en el caso de *cloud computing*. Estos servidores y los servicios asociados pueden tener distintas sedes nacionales, pudiendo estar los datos en más de un país. Los tratamientos transfronterizos de datos personales de personas que residen en el país y su alojamiento en países distinto a Chile plantean un desafío para la vigencia de los derechos de los titulares de datos y para hacer exigibles las obligaciones que establece la ley, respecto de los responsables del tratamiento de datos.

Dado el actual desarrollo tecnológico y de Internet, así como la expansión del *cloud computing*, se requiere asegurar que el régimen regulatorio que busca sustituir a la Ley N° 19.628 tenga plena vigencia, incluso para tratamientos transfronterizos de datos personales. En ese orden de cosas, resulta fundamental que toda regulación en materia de protección de datos incorpore, dentro de su ámbito de aplicación, la extraterritorialidad de la ley. Sin embargo, ninguna de las iniciativas legislativas en curso aborda este importante aspecto.

En consecuencia, es que se sugiere que se establezca explícitamente una regla de extraterritorialidad de la legislación de protección de datos personales, siguiendo los estándares de la Unión Europea, en base a los siguientes criterios:

- Cuando el tratamiento por un mandatario se efectúa fuera del territorio nacional a nombre de un responsable establecido o constituido en Chile.
- Cuando se traten datos personales fuera del territorio para ofrecer bienes o servicios dentro de Chile.
- Cuando le resulte aplicable por normas y tratados internacionales.

Propuesta de ámbito de aplicación de la ley
La presente ley se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en el territorio nacional, independientemente de que el tratamiento tenga lugar en Chile o no. *Asimismo, se aplica al tratamiento de datos personales de titulares que residan en Chile por parte de un responsable o encargado no establecido en el territorio nacional, en los siguientes casos:* *a) Si el tratamiento es efectuado por un mandatario fuera del territorio nacional a nombre de un responsable establecido o constituido en Chile.* *b) Si se tratan datos personales fuera del territorio de la República con el fin de ofrecer bienes o servicios a dichos titulares dentro de Chile, y* *b) Cuando así se disponga en normas o tratados internacionales ratificados Chile y que se encuentren vigentes.*

c. **Excepciones a la aplicación de la ley.** La modificación de la Ley N° 19.628 supone el reemplazo de la actual regla general y de clausura en materia de protección de datos personales. En este sentido, al tratarse de un régimen general, varias materias quedarían reguladas bajo normas especiales o excepcionales. La misma modificación a la Ley N° 19.628 debiese consagrar un limitado régimen de excepciones, puesto que el estándar de protección de los datos personales –actualmente en Chile– es demasiado bajo y cualquier ámbito que se margine de la aplicación de la norma general contaría con una protección deficitaria.

En lo relativo a las excepciones a la aplicación de este régimen regulatorio, el Proyecto del Ejecutivo excluye el tratamiento de datos que realicen los medios de comunicación 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, y al que efectúen las personas naturales en relación con sus actividades personales. La Moción, por su parte, excluye de la regulación los datos personales almacenados en bases de datos domésticas y para actividades relacionadas con su vida privada y familiar.

El Proyecto del Ejecutivo, en cambio, excluye de la aplicación de la ley **todo** tratamiento de datos que realicen los medios de comunicación en el ejercicio de las libertades de emitir opinión y de informar referidas en el artículo 19 N° 12 de la Constitución, sin excepciones, sino que además considera un régimen de excepciones en su artículo 24, que incluye el tratamiento de datos para la investigación, persecución, enjuiciamiento o sanción de infracciones penales, civiles y administrativas, y en el evento que se declaren estados de catástrofe o emergencia, entre otros. Como se puede advertir, el catálogo de excepciones que propone el Proyecto del Ejecutivo es sumamente amplio.

Propuesta: Sobre la base de lo anterior, se sugiere lo siguiente:

- Acotar las excepciones a las bases de datos domésticas vinculadas a la vida familiar y a aquellas que regulen las leyes a que se refiere el artículo 19 Nº 12 de la Constitución Política de la República, excluyendo a los medios de comunicación que mantengan bases de datos para finalidades distintas a las de opinar e informar, tales como las bases de datos de clientes y personal.

Propuesta de excepciones a la aplicación de la 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.*

2. Definiciones y principios

a. Definiciones. Si bien la Ley Nº 19.628 contempla un catálogo de definiciones, éstas se encuentran actualmente superadas y varias de ellas han demostrado su insuficiencia, en términos de certeza jurídica, para la aplicación de los derechos y obligaciones consagrados en el citado cuerpo legal. Ambas iniciativas legislativas reemplazan y se actualizan los conceptos de la ley, además de la incorporación otros nuevos.

El Proyecto del Ejecutivo define cada uno de los llamados derechos ARCO (de acceso, rectificación, cancelación y oposición). Pero carece de ciertas definiciones, tales como transferencia internacional de datos, encargado o intermediario del tratamiento, motor de búsqueda, entre otras. Además, el proyecto, por ejemplo, propone una nueva definición de fuente de acceso público pero que entrega a la nueva Agencia de Protección de Datos Personales, ante la duda, la determinación final de cuáles son las fuentes. Esta definición, por lo tanto, deja abierta el contenido del concepto y abre la posibilidad de eventuales conflictos en la aplicación de las reglas de transparencia y acceso a la información pública.

La Moción, por su parte, no define los derechos ARCO. Incorpora conceptos de transmisión internacional de datos o encargado del tratamiento de datos, a diferencia del Proyecto del Ejecutivo. Además define de manera taxativa que se entiende por fuentes de acceso público y lo vincula en su caso, a una contraprestación económica.

En materia de datos sensibles, existe una omisión en ambos proyectos de ley: se suprime la referencia a los “hábitos personales” que actualmente establece el artículo 2, letra g) de la Ley N° 19.628. Esta omisión constituye un evidente retroceso del estándar legal vigente en la materia. Por ello, este factor debe ser necesariamente incorporado en los proyectos de ley que actualmente se encuentran en tramitación.

Propuesta: Sobre la base de los antecedentes expuestos, es que se sugiere lo siguiente:

- **Dato personal.** Se sugiere seguir la definición que al respecto propone el Reglamento de Protección de Datos de la Unión Europea[3] (en adelante, “Reglamento Europeo”), al definir qué se entiende por persona identificable. En esta materia, se podría incorporar explícitamente cuándo una persona es “identificable”, entregando ejemplos para ello.
- **Datos sensibles.** Se propone seguir el estándar europeo en esta definición, integrando categorías ampliamente aceptadas en el derecho comparado (por ejemplo, incorporando el factor de afiliación sindical). Un elemento fundamental de la definición supone vincular el

[3] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 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 por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

tratamiento de datos sensibles con una eventual discriminación arbitraria e ilegal o que conlleve un grave daño para el titular. Por otro lado, no se entiende por qué ambos proyectos han eliminado el factor de "hábitos personales" dentro de la definición de datos sensibles, considerando que ambos proyectos buscan elevar el estándar garantista y que las principales discriminaciones se dan en función de los hábitos de las personas.

- **Fuente de acceso público.** Se sugiere descartar la técnica regulatoria del Proyecto del Ejecutivo, que deja en manos de la Agencia la determinación *in concreto* de cuáles son fuentes de acceso público y cuáles no. Esto produciría en la práctica una indeterminación del contenido del concepto, dejando la puerta abierta para futuros problemas de interpretación. En concreto, con la definición actual de fuentes de acceso al público, el Consejo ha tenido que conocer de casos en los que se discute si un determinado registro público tiene la calidad de fuente de acceso al público, con la consiguiente dificultad de resolver caso a caso. En ese sentido, para dar solución a dicha problemática, se propone seguir la técnica taxativa de enumerar las fuentes de acceso al público, siguiendo en este punto lo propuesto por otras legislaciones más avanzadas en la materia, como la española, plasmada en su Ley Orgánica de Protección de Datos, con su respectivo reglamento[4]. Asimismo, por tratarse de datos estadísticos, y no datos personales, se incorpora la información proveniente del Censo de Población y Vivienda y de la Encuesta y la Encuesta de Caracterización Socioeconómica Nacional. En estos casos, no se trata

[4] Artículo 3, letra j) de la Ley Orgánica de Protección de Datos de España: Fuentes de Acceso Público: "*Aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y 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. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.*"
A su vez, el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal de España, dispone lo siguiente: Artículo 7. Fuentes accesibles al público.
1. A efectos del artículo 3, párrafo j) de la Ley Orgánica 15/1999, se entenderá que sólo tendrán el carácter de fuentes accesibles al público:
a) El censo promocional, regulado conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre.
b) Las guías de servicios de comunicaciones electrónicas, en los términos previstos por su normativa específica.
c) Las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección profesional e indicación de su pertenencia al grupo. La dirección profesional podrá incluir los datos del domicilio postal completo, número telefónico, número de fax y dirección electrónica. En el caso de Colegios profesionales, podrán indicarse como datos de pertenencia al grupo los de número de colegiado, fecha de incorporación y situación de ejercicio profesional.
d) Los diarios y boletines oficiales.
e) Los medios de comunicación social.
2. En todo caso, para que los supuestos enumerados en el apartado anterior puedan ser considerados fuentes accesibles al público, será preciso que su consulta pueda ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación.

de datos personales, en sentido estricto, puesto que a través de tratamientos de disociación o anonimización, el dato es estadístico y constituye información de fuente de acceso público.

- **Proceso de disociación o anonimización.** La definición del Proyecto del Ejecutivo resulta más precisa, desarrollando en términos amplios el procedimiento de disociación de datos. Sobre esa base, se propone tomar como base la definición del Ejecutivo, y complementar con la Moción en lo que se refiere a las "*medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuya a una persona natural identificada o identificable*", por cuanto sigue el estándar definido en el Reglamento europeo de Protección de Datos.
- **Incorporar definiciones.** Se propone incorporar definiciones de "Encargado" y "Motor de búsqueda" del tratamiento de datos, en línea con la tendencia europea en la materia. En ese sentido, resulta relevante destacar lo resuelto por la jurisprudencia del Tribunal Europeo[5], la cual ha determinado que los motores de búsqueda, como intermediarios en el tratamiento, efectúan almacenamiento y procesamiento de datos para efectos de generar los resultados. Se propone redactar definiciones de dato "relativo a la salud", dato "genético" y dato "biométrico" en base a la noción conceptual de la Moción pero con los ejemplos de los arts. 16 bis, 16 ter y 16 quater del Proyecto del Ejecutivo.

Propuesta de definiciones
Dato personal: *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 y excluyendo aquellos casos en que el esfuerzo de identificación sea desproporcionado.* ***Dato sensible:*** *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, los hábitos personales, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, los datos relativos a la salud, la vida u orientación sexual, hábitos personales, los datos genéticos, biométricos, entre otros.* ***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*

[5] Sentencia del TJEU sobre la interpretación de los artículos 2, letras b) y d), 4, apartado 1, letras a) y c), 12, letra b), y 14, párrafo primero, letra a), de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281, p. 31), y del artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, en caso Google Spain, S.L. y Google Inc. contra la Agencia Española de Protección de Datos y el Sr. Mario Costeja González.

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.
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; porque dicha asociación exige un esfuerzo no razonable, entendiendo por tal el empleo de una cantidad de tiempo, gasto o trabajo desproporcionados, o porque se ejercieron medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona natural identificada o identificable. Un dato anonimizado deja de ser un dato personal.*
Encargado del tratamiento o encargado: *la persona natural o jurídica que trate datos personales por cuenta del responsable del tratamiento.*
Motor o mecanismo de búsqueda: *Persona natural o jurídica dedicada a la actividad de buscar información publicada o puesta en Internet, anexarla o indexarla de manera automática, almacenarla temporalmente y ponerla a disposición de las personas según un orden de preferencia determinado. Esta actividad se considerará siempre como tratamiento de datos personales y quien efectúe dicho tratamiento será considerado responsable para todos los efectos legales.*
Datos relativos a la salud: *datos personales relativos a la salud física o mental de una persona natural, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.*
Datos genéticos: *datos personales relativos a las características genéticas heredadas o adquiridas de una persona natural que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.*
Datos biométricos: *datos personales obtenidos a partir de un tratamiento técnico especifico, relativos a las características físicas, fisiológicas o conductuales de una persona natural que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.*

b. Principios. El crecimiento de la regulación en materia de protección de datos y la diversidad de ámbitos en que sus reglas deben ser aplicadas, ha generado la necesidad de establecer orientaciones interpretativas a través de principios. Los principios al interior de las leyes, como en el caso de la Ley de Transparencia, constituyen un insumo fundamental a la hora de orientar y concretizar mandatos generales y fijar directrices interpretativas de la legislación. En la materia de protección de datos, el referente se encuentra en los desarrollos del nuevo Reglamento Europea, que incorpora un

omnicomprensivo catálogo de principios. De la misma forma, la OCDE también ha generado un catálogo de principios de protección de datos personales..

El proyecto del Ejecutivo establece un listado acotado de siete principios: licitud del tratamiento; finalidad; proporcionalidad; de calidad; responsabilidad; seguridad e información. Otros principios no recogidos por el mensaje, como el de información y transparencia o de seguridad, los establece como deberes para el responsable del tratamiento (artículos 14 ter y 14 quáter).

La Moción propone un catálogo más amplio de principios, incorporando el de confidencialidad, transparencia, minimización de datos, temporalidad, o responsabilidad y rendición de cuentas.

La legislación actual carece de un catálogo de principios que estén explícitamente establecidos como tal y sólo se reconocen a partir de ciertas reglas. Por ello, ambas propuestas significan un avance en la materia al incorporarlos y, además, en coincidir en la gran mayoría de ellos.

Propuesta: En consideración a estos elementos, se sugiere lo siguiente:

- **Principio de finalidad.** El proyecto del Ejecutivo no considera como excepción a este principio el uso posterior de los datos con fines de archivo, fines de investigación científica e histórica o fines estadísticos, tal como lo propone el Reglamento Europeo.
- **Proporcionalidad.** Se propone fusionar la propuesta conceptual de la Moción con el agregado del Proyecto del Ejecutivo respecto de la conservación limitada en el tiempo y disponiendo la cancelación o anonimización de los datos cuando la finalidad del tratamiento ya ha sido cumplida, permitiendo de esta forma concretizar los requerimientos de plazos y forma que exige la proporcionalidad.
- **Calidad.** El Proyecto del Ejecutivo se centra en la exactitud de los datos y su actualidad, pero no considera la exigencia de adoptar todas las medidas razonables de suprimir o rectificar los datos cuando éstos no cumplan con tal fin de exactitud, tal como prescribe el Reglamento Europeo.
- **Responsabilidad.** El Proyecto del Ejecutivo exige que el responsable del tratamiento de datos sea capaz de demostrar el cumplimiento de la ley. Esta exigencia permite acotar, de mejor forma, el alcance del principio y darle un contenido cierto.
- **Seguridad**. Si bien ambas definiciones son similares, se sugiere seguir el Proyecto del Ejecutivo, ya que incorpora la hipótesis de “filtración” como posible afectación del principio.
- **Información.** Se propone seguir la formulación de la Moción, con la exigencia adicional de “gratuidad” del Proyecto del Ejecutivo.

Propuesta de principios

Principio de finalidad: *Los datos solo serán tratados con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; el tratamiento posterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales.*

Principio de proporcionalidad: *El tratamiento de datos personales deberá circunscribirse a aquellos 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.*

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 al necesario, requerirá autorización legal o consentimiento del titular, en los términos de esta ley.

Principio de 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.*

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, debiendo ser capaces de demostrarlo.*

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.*

Principio de información: *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, niña o adolescente. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos.*

3. Consentimiento, datos sensibles y datos especialmente protegidos

a. Consentimiento. El consentimiento es fuente de legitimidad del tratamiento de los datos personales. En ese sentido, ambas propuestas normativas incorporan este elemento esencial de toda legislación sobre protección de datos personales. En base a esta fuente de legitimidad, los datos personales deben mantenerse en la esfera de control de su titular. Ambas propuestas coinciden en señalar que el consentimiento constituye la fuente principal de legitimidad del tratamiento de datos.

En esa línea, el Proyecto del Ejecutivo dispone que el consentimiento es una de las dos fuentes de licitud para el tratamiento de datos personales, junto a la misma ley. Además, supedita el consentimiento al principio de finalidad y asigna la carga de la prueba del consentimiento al responsable del tratamiento.

La Moción, por su lado, establece que el consentimiento no es válido si existe una asimetría clara entre el titular y el responsable del tratamiento y, además, asigna que la carga de la prueba del consentimiento recaiga en el responsable.

Ambas iniciativas coinciden en cuanto a describir las características principales del consentimiento, como la de ser libre, inequívoco e informado, y en cuanto a que puede ser revocado sin expresión de causa, utilizando técnicas o medios similares a aquellos a través de los cuales lo otorgó y sin que tenga efectos retroactivos.

Propuesta: La formulación del consentimiento debe contemplar sus elementos centrales: libre, informado, inequívoco, específico en cuanto a su finalidad y previo, así como asegurar siempre la facultad de revocación.

- Ambas propuestas contemplan las exigencias de los medios para otorgar o revocar el consentimiento.
- Se sugiere, además, incorporar la regla de interpretación sobre si el consentimiento ha sido libre en el caso de situaciones de “desequilibrio claro entre la posición del titular y responsable”, contenida en la Moción.

Propuesta de regla general de consentimiento
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 o lo autorice la ley. *El consentimiento del titular debe ser libre e informado, otorgarse en forma previa al tratamiento y debe ser específico en cuanto a su finalidad o finalidades. Debe manifestarse de manera inequívoca, mediante una declaración verbal, escrita o realizada a través de un medio electrónico equivalente o mediante un acto afirmativo que dé cuenta con claridad de la voluntad del titular.* *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.* *Cuando el consentimiento lo otorgue un mandatario, éste 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 tiene 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.
Corresponde al responsable probar que el tratamiento de datos realizado contó con el consentimiento del titular o fue efectuado por disposición de la ley.

b. Excepciones al consentimiento. Las excepciones al consentimiento son una de las materias más delicadas de la regulación de protección de datos personales. Por un lado, éstas deben permitir armonizar el tratamiento de datos para alcanzar finalidades legítimas y autorizadas por la ley mientras que, por otra parte, las excepciones no pueden terminar afectando este principio general de legitimidad en el tratamiento de datos. Las excepciones deben ser fijadas por la ley de la forma más clara y precisa posible, con el fin de proteger la autodeterminación informativa y evitar distorsiones respecto de la voluntad del titular de los datos. Ambos proyectos actualizan y precisan de mejor manera estas excepciones, superando la actual regulación establecida en el artículo 4º de la Ley Nº 19.628.

El Proyecto del Ejecutivo dispone un estatuto que fija las siguientes excepciones: 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.

La Moción, por su parte, permite la cesión de datos sin consentimiento cuando esté autorizada en una ley; cuando 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; cuando la cesión se produzca entre órganos del Estado en el ejercicio de sus atribuciones y el tratamiento de los datos tenga fines históricos, estadísticos o científicos.

Propuesta: Respecto del contenido de las excepciones, se propone lo siguiente:

- Las fuentes de acceso público pueden ser una excepción al consentimiento **sólo si se sigue la definición dado por el estándar europeo en la materia** y no en base al modelo del Proyecto del Ejecutivo.
- Incorporar la excepción para el cumplimiento de obligaciones legales o contractuales en la que es parte el titular, pero agregando la exigencia de finalidad que le sirve de causa a la obligación.
- Se pueden incorporar excepciones acotadas tales como aquellas con datos disociados con fines estadísticos, históricos o científicos.

Propuesta de excepciones al consentimiento
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 de aquellas taxativamente establecidas en la presente ley.* *b) 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, y éste se relacione con los fines del tratamiento.* *c) 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 los datos se encuentren debidamente disociados.*

c. Datos sensibles. La regulación de datos sensibles es uno de los puntos de mayor relevancia, ya que buscan proteger a personas o grupos de personas que por su condición o características, pueden ser objeto de una eventual discriminación o un daño futuro. Junto con mejorar las reglas del tratamiento de los datos sensibles, se debe tener presente las propuestas de mejoras a la definición de este concepto, con el objeto de evitar que se omitan a los "hábitos personales" como parte de lo protegido.

El Proyecto del Ejecutivo lo regula a través de una definición que mejora y actualiza la vigente en la Ley Nº 19.628, y regula este aspecto vinculando el dato sensible con las características físicas o morales de una persona, enunciando algunas como el origen racial, ideología, afiliación política, creencias o convicciones religiosas, entre otras.

A diferencia del mensaje, la Moción establece que el dato sensible (o especialmente protegido), es aquel cuyo tratamiento pueda dar origen a una discriminación arbitraria o ilegal o que conlleve un grave riesgo para su titular, enunciando también una serie datos que puedan caer dentro de esta categoría, tales como los datos de niños y niñas, aquellos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas.

Como se puede apreciar, ambos conceptos definen al dato sensible desde dos miradas distintas. El Proyecto del Ejecutivo, desde la óptica de las características de la persona. En cambio, la Moción la regula y define a partir de las consecuencias que puede traer aparejado el tratamiento para una determinada persona, siguiendo en este punto el estándar europeo en la materia.

Propuesta: En consecuencia, se propone seguir el estándar europeo, que se recoge en la Moción. Respecto del tratamiento de datos sensibles, se sugiere lo siguiente:

- Sólo podrá hacerse cuando exista consentimiento previo y, además, **explícito** por parte del titular.

- Se propone seguir las excepciones del estándar del Reglamento Europeo, el cual enumera taxativamente aquellos casos en que puede exceptuarse el consentimiento para datos especialmente protegidos, dentro de los cuales pueden citarse a modo ejemplar, entre otros: cuando resulte necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento.

Propuesta de regulación de tratamiento de datos sensibles
Regla general para el tratamiento de datos sensibles. El tratamiento de los datos 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. *Lo dispuesto en el inciso anterior no será aplicable en las siguientes circunstancias:* *a) 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.* *b) 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.* *c) 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.* *d) El tratamiento se refiera a datos personales que el titular haya hecho voluntariamente públicos;* *e) El tratamiento sea necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial.* *f) El tratamiento sea realizado por un organismo público en el cumplimiento de una obligación legal.*

4. Derechos ARCO

En toda regulación sobre protección de datos personales, tiene un papel preponderante la normativa relativa a los llamados Derechos ARCO (derechos de acceso, rectificación, cancelación y oposición). Se tratan de facultades inherentes a la autodeterminación informativa y constituyen una herramienta eficaz para la protección del titular de los datos ante el responsable del tratamiento.

El derecho de acceso se entiende como aquel que permite a una persona obtener del responsable del tratamiento la confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, acceder a los mismos. El derecho de rectificación es aquel que permite al titular obtener del responsable del tratamiento la corrección de los datos personales inexactos que le conciernan. El derecho de cancelación es aquel que autoriza a una persona, obtener la supresión o eliminación de los datos personales que le conciernan, sin dilación indebida del responsable del tratamiento. El derecho de oposición, finalmente, es aquel que permite a una persona, oponerse al tratamiento de sus datos personales, cuando concurra una razón derivada de su situación personal o bajo otros supuestos que la ley así los contemple.

Si bien la Ley Nº 19.628 considera estos derechos –con excepción del derecho de oposición– no los regula de manera sistematizada y coherente. En efecto, la actual normativa los establece en el Título II de la citada ley, como parte de los "Derechos de los Titulares de los Datos", sin enunciar ni separar cada uno de estos importantes derechos.

Ambos proyectos de ley consideran una regulación especial de los derechos ARCO. Además, el Proyecto del Ejecutivo incorpora cada derecho al catálogo de definiciones, así como el derecho a la portabilidad de los datos, en virtud del cual el titular de datos puede solicitar y obtener del responsable, una copia de sus datos personales y comunicarlos o transferirlos a otro responsable de datos. Este último resulta una innovación respecto a lo planteado por la Moción, ya que el Reglamento de la UE considera y regula dentro del catálogo de derechos de los titulares.

La Moción, por su parte regula de manera diferenciada cada uno de estos derechos, siguiendo muy de cerca el estándar europeo plasmado en el Reglamento de la Unión Europea sobre Protección de Datos Personales.

Propuesta: Como se señaló, si bien ambas propuestas normativas consideran una regulación especial para estos derechos, se sugiere lo siguiente:

a. En términos generales, se propone que se regule explícitamente que todos los derechos ARCO sean **gratuitos,** con el fin de permitir que estos derechos puedan ser ejercidos por la totalidad de los ciudadanos. La exigencia de una contraprestación pecuniaria por parte del responsable o encargado, resultaría en la práctica, en una barrera para poder ejercer algunos de estos derechos.

b. **Derecho de acceso.** Se sugiere seguir la regulación del Proyecto del Ejecutivo, que contiene un mayor detalle de los contenidos mínimos que deben ser informados al titular del dato, tales como los datos tratados y su origen; la finalidad o finalidades del tratamiento; las categorías, clases o tipos de

destinatarios a los que se han comunicado o cedido los datos o se prevé comunicar o ceder, o el período de tiempo durante el cual los datos serán tratados. Además, regular los casos en que el responsable no estará obligado a entregar la información al titular.

c. **Derecho de rectificación.** Se sugiere seguir la regulación del Proyecto del Ejecutivo, el cual añade al requerimiento que el dato sea inexacto, incompleto o desactualizado, la obligación de que el contenido sea público, debiendo difundirse cuando así lo requiera el titular y sea necesario para los fines del tratamiento. En ese mismo sentido, se propone incorporar las hipótesis de datos "innecesarios o excesivos" de la Moción.

d. **Derecho de cancelación.** Se sugiere seguir el estándar europeo, el cual lo regula como el derecho a obtener sin dilación indebida del responsable del tratamiento la cancelación o supresión de los datos personales que le conciernan. Sin embargo, se propone complementar este punto con lo propuesto por el Ejecutivo, el cual regula las excepciones a este derecho, de forma expresa, al igual que lo hace el Reglamento de la Unión Europea.

e. **Derecho de oposición.** Se sugiere seguir el estándar europeo, el cual dispone que el interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular. Además, el Reglamento Europeo regula la oposición que pueda hacer el titular respecto al tratamiento de datos con fines de mercadotecnia, optando por la figura de darle al interesado, en la primera comunicación, el derecho a oponerse con el fin de quedar al margen de cualquier otra información futura.

   En ese sentido, en el caso de la cancelación respecto de datos tratados con fines de comunicaciones comerciales o publicitarias (a propósito del proyecto "No Molestar"), se propone seguir el Proyecto del Ejecutivo –que exige un contrato entre las partes para ese tratamiento–, a diferencia de la Moción, que dispone la regla de las listas de exclusión.

f. **Derecho de portabilidad de los datos.** Se estima una buena innovación de ambos proyectos, debiendo considerarse la entrega de los datos al titular y garantizar el traspaso directo de un responsable a otro, en ambos casos, de forma gratuita para el titular.

Propuesta de derechos ARCO
Derechos de los titulares 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, oposición y de portabilidad son personales, intransferibles e irrenunciables, de carácter gratuito, y no pueden limitarse por ningún acto o convención*
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, sus categorías 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.*
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, incompletos, innecesarios o excesivos. *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.*
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.*
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) 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. *f) Los datos sean usados para la elaboración de perfiles.*
Derecho a la portabilidad de datos. 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 directamente a otro responsable de datos.

5. Responsable y encargado

a. Aspectos generales. En general, las regulaciones sobre tratamientos de datos, aspiran a regular tanto los derechos del titular, como los deberes y obligaciones de quienes tratan los datos. La determinación de un régimen de responsabilidad permite distribuir los riesgos asociados al tratamiento de datos. Las obligaciones permiten ajustar la conducta tanto de los responsables como de los encargados en el tratamiento de datos personales. Asimismo, permiten equilibrar la asimetría entre éstos y el titular, cuestión que adquiere más importancia como consecuencia del desarrollo masivo de las comunicaciones y la interconexión tecnológica actual, entre otros aspectos.

En ese sentido, tanto el Proyecto del Ejecutivo como la Moción, se hacen cargo de regular separadamente las obligaciones que pesan sobre los responsables y encargados del tratamiento de los datos.

El Proyecto del Ejecutivo dispone de un régimen de responsabilidades de los responsables de datos, entre los que se destaca la creación de una serie de obligaciones y deberes, tales como:

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: es decir, un deber de información oportuno ante la solicitud del titular, de que el tratamiento de datos se funda en alguna causa que lo valide.

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: el responsable debe cumplir con el principio de finalidad propuesto en el proyecto.

c) Comunicar o ceder, información exacta, completa y veraz: lo cual debe realizarse cumpliendo con los requisitos y condiciones que el mismo proyecto propone.

d) Cumplir con los demás principios que rigen el tratamiento de los datos personales previstos en esta ley: lo cual le da un valor directo y concreto a los principios enumerados en el proyecto, ya no solo con un fin

interpretativo o de orientación, sino como una obligación legal, a lo cual el responsable debe atender.

Además, establece 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. No define la figura del encargado, aunque si regula sus obligaciones.

La Moción, por su parte, regula tanto los deberes y obligaciones del responsable como los del encargado del tratamiento, estableciéndose el deber hacia ellos de llevar un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Asimismo, fija un contenido mínimo para las reglas contractuales que rijan en la relación entre el responsable y el encargado del tratamiento de datos personales.

Propuesta: Basado en lo anteriormente expuesto, es que se sugiere lo siguiente:

- Se sugiere incorporar una definición de “Encargado” o “Mandatario” en el tratamiento de datos personales. En ese sentido, se sugiere la siguiente redacción:
- **Encargado.** La persona natural o jurídica que trate datos personales por cuenta y conforme las instrucciones que le imparta el responsable, quedándole prohibido su tratamiento, cesión o entrega para un objeto distinto del convenido con el responsable.
- **Responsable.** Se sugiere seguir el Proyecto del Ejecutivo, que detalla y regula en extenso los deberes y obligaciones del responsable en el tratamiento de datos personales.
- Se sugiere incorporar la obligación de **registrar los bancos de datos ante la Autoridad de Control**, con el objeto de fomentar una concientización de los deberes asociados al tratamiento de datos personales.
- Se sugiere especificar los deberes que tiene el responsable en relación al mandatario, en el tratamiento de datos personales.

Propuesta de reglas en materia de responsable de tratamiento de datos
Definición de encargado. La persona natural o jurídica que trate datos personales por cuenta del responsable del tratamiento.
Definición de motor o mecanismo de búsqueda: Persona natural o jurídica dedicada a la actividad de buscar información publicada o puesta en Internet, anexarla o indexarla de manera automática, almacenarla temporalmente y ponerla a disposición de las personas según un orden de preferencia determinado. Esta actividad se considerará siempre como tratamiento de datos personales y quien efectúe dicho tratamiento será considerado responsable para todos los efectos legales
Deberes generales del responsable y el encargado de tratamiento de datos. El

responsable y el encargado 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) Llevar un registro de las actividades de tratamiento efectuadas bajo su responsabilidad.
e) Cumplir con los demás principios que rigen el tratamiento de los datos personales previstos en esta ley.

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.

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.

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.* *Deber de reportar las vulneraciones a las medidas de seguridad. El responsable de datos debe reportar a la autoridad de control, 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*
Registro de las bases de datos. La autoridad de control llevará un registro de las bases de datos personales a cargo de los responsables del tratamiento de datos personales, cuando traten datos sensibles, cuyos responsables sean órganos del estado, y en el caso de empresas que presten servicios de utilidad pública y en los demás casos que la autoridad de control defina por resolución fundada. *Este registro tendrá carácter público y en él constará, respecto de cada una de esas bases 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 deberá ser regulado en un reglamento.* *El responsable de la base de datos proporcionará esos antecedentes a la autoridad de control cuando se inicien los tratamientos de la base y deberá comunicar cualquier cambio de los elementos indicados en el inciso anterior dentro de los quince días desde que se produzca.* *La infracción a este artículo será sancionado conforme a las reglas de las infracciones leves a que se refiere el artículo XXX.*

b. **Encargado o mandatario.** Se sugiere definir y regular, separadamente, sus obligaciones, con independencia de la figura del responsable, tal como lo regula el Reglamento Europeo sobre Protección de Datos. En esa línea se propone la siguiente redacción:

- **Deberes del encargado**: El tratamiento de datos por parte del encargado se regirá por un contrato suscrito entre éste y el responsable, en el cual se establecerá el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Asimismo, dicho contrato deberá contener los siguientes deberes para el encargado, entre otros:

  a) Tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional.

  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.

  c) Tomará todas las medidas necesarias de seguridad.

  d) Asistirá al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados.

  e) A elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento.

  f) Pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

Propuesta en materia de encargado de tratamiento de datos
Deberes del encargado. El responsable del tratamiento 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 o devolverá todos los datos personales una vez que finalice la prestación de los servicios de tratamiento, y cancelará las copias existentes a menos que se requiera la conservación de los datos personales en virtud de la ley;

f) pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

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

c. **Diferenciación de estándares.** Si bien es razonable establecer criterios para diferenciación de estándares entre grandes y pequeños tratadores de datos, los criterios de ambos proyectos no son suficientes. La Moción opta por un criterio numérico (organizaciones de menos de 200 personas) más un criterio correctivo de riesgo para las libertades y derechos de las personas. El Proyecto del Ejecutivo opta simplemente por un criterio legal, esto es, las empresas de menor tamaño según la Ley N° 20.416, y su posterior regulación por un Reglamento.

- Se propone distinguir entre personas naturales y jurídicas. Las primeras debiesen tener un bajo estándar de cumplimiento, salvo que traten datos personales sensibles y especialmente protegidos y no sólo una alusión al riesgo de derechos y libertades.
- Las personas jurídicas que sean susceptible de clasificación bajo la Ley N° 20.416, tendrán un estándar diferenciado en los siguientes términos:
    - Las microempresas deberían tener un bajo estándar de cumplimiento de obligaciones.
    - Las pequeñas empresas deberían tener un mediano estándar de cumplimiento de obligaciones.
    - Las empresas medianas y grandes deberían tener un alto estándar de cumplimiento de obligaciones.
- Se propone que, en todo caso, siempre se aplicará un alto estándar de cumplimiento cuando el tratamiento se refiera a datos sensibles y especialmente protegidos. Esto debiese regir tanto para personas naturales como jurídicas.
- Se propone que sea la Autoridad de Control la que, a través de sus facultades regulatorias, determine en concreto las instituciones que tendrán un estándar diferenciado de cumplimiento.

Propuesta en materia de 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, serán determinados por la autoridad de control, considerando los siguientes factores: *a) Las personas naturales tendrán un bajo estándar de cumplimiento, salvo que traten datos personales sensibles y especialmente protegidos.* *b) En el caso de las personas jurídicas, el estándar de cumplimiento será diferenciado en función de las categorías de empresas conforme a la Ley N° 20.416. Las microempresas tendrán un bajo estándar de cumplimiento de obligaciones. Las pequeñas empresas tendrán un mediano estándar de cumplimiento de obligaciones. Las empresas medianas y grandes tendrán un alto estándar de cumplimiento de obligaciones.* *En todo caso, siempre se deberá aplicar un alto estándar de cumplimiento cuando el tratamiento se refiera a datos sensibles y especialmente protegidos o cuando el tratamiento que realice el responsable pueda producir un riesgo para los derechos o libertades de los titulares.*

6. Regulación de las competencias de los órganos del Estado

Junto al consentimiento, la otra fuente de legitimidad para el tratamiento de los datos personales es la ley. La ley constituye un título legítimo para el tratamiento de datos personales. En el sector público, la ley constituye fundamento y medida para el tratamiento de datos. Por ello, los organismos públicos puedan tratar datos personales siempre circunscritos al ámbito de sus facultades y competencias tipificadas en la ley, sin el consentimiento del titular.

El Proyecto del Ejecutivo propone, en este ámbito, regular 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. Además, establece que estos organismos pueden comunicar o ceder datos personales cuando se requieran para un tratamiento que tenga por finalidad otorgar beneficios al titular, evitar duplicidad de trámites o reiteración de requerimientos de información o documentos para los titulares.

La Moción, en un sentido similar, plantea que estos organismos pueden ceder los datos personales que tratan, a otros órganos del Estado con el fin 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. Sin embargo, por razones de iniciativa exclusiva del Presidente de la República, en materia de ley, la Moción no profundiza en la regulación de las competencias de los órganos públicos.

Propuesta: En base a lo anteriormente expuesto, se propone lo siguiente:

- Debe quedar claramente establecido que dicho tratamiento sólo se podrá efectuar respecto de materias de su competencia, regulando la forma y condiciones que
- los órganos del Estado mantendrán bases de datos. Ambos proyectos satisfacen dicho estándar.
- Debe suprimirse alusión al art. 20 de la Ley de Transparencia, puesto que carece de contexto en materia de protección de datos personales. Los derechos de las personas no se refieren necesaria o exclusivamente a derechos a la protección de datos personales. Por lo tanto, al remitirse a la Ley Nº 20.285, el Proyecto del Ejecutivo confunde las reglas aplicables a la comunicación de datos entre organismos públicos y la transparencia o secreto de los derechos de terceros. En efecto, la disposición del artículo 21 Nº 2 de la Ley de Transparencia apela a aspectos que van más allá tales como la seguridad, salud o derechos de carácter comercial o económico, siendo la protección de datos un elemento que puede entenderse subsumido dentro del catálogo de derechos que aspiran proteger y garantizar las normas de la citada ley. Por otro lado, los organismos públicos sí pueden transferir o comunicar datos personales que puedan ser reservados; ello podría, eso sí, tener consecuencias en los deberes de seguridad y confidencialidad del responsable del tratamiento. Entonces, debiese regularse en tal sentido y no efectuar una remisión a la Ley de Transparencia.
- **Comunicación e interoperabilidad.** Respecto de la comunicación o cesión de datos, si bien ambos proyectos establecen las dos exigencias básicas –que la comunicación

sea necesaria para el cumplimiento de una función legal y dentro de las competencias de cada órgano, así como para efectos de prestar servicios o evitar la duplicación de trámites respecto del titular– no parece conveniente que el Proyecto del Ejecutivo permita cesiones "indefinidas", sino que éstas deben sujetarse, al menos, al cumplimiento de la finalidad prevista.

- **Datos relativos a infracciones penales, civiles, administrativas y disciplinarias**. En esta materia, se sugiere seguir la fórmula del Proyecto del Ejecutivo. Se sugiere que, conforme a la jurisprudencia constante de los tribunales superiores de justicia, se exceptúe de la prohibición de comunicación la sentencia judicial o el acto administrativo fundante que dispone la sanción.

Propuesta de regulación de los órganos del Estado
Tratamiento de datos personales por parte de los organismos públicos. 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 información y seguridad que deba adoptar y el cumplimiento de las demás obligaciones de la presente ley.*
Comunicación e interoperabilidad. 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.*
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, así como de las sentencias judiciales o actos administrativos fundantes que dispusieron la sanción.

7. Transferencia internacional de datos personales

Los flujos transfronterizos de datos a nivel internacional resultan, hoy, fundamentales tanto para el desarrollo del comercio como para la cooperación internacional. Para efectuar tales tratamientos, los Estados requieren de regulaciones adecuadas y actualizadas que garanticen, por un lado, la protección de los datos personales y, por el otro, habiliten una fluida comunicación de éstos entre distintos Estados. Si bien en esta materia se requiere una coordinación entre los países, cada Estado, además, debe proteger los datos que traspasan sus fronteras.

Este aspecto no es tratado en detalle por la Moción, pese a que define el concepto. Lo anterior se explica en que se trata de una materia de iniciativa exclusiva del Presidente de la República y, por lo tanto, escapa de la esfera de competencia de los parlamentarios.

La transferencia internacional sí es regulada por el Proyecto del Ejecutivo, el cual autoriza como regla general, la transferencia internacional de datos, pero sólo con aquellos países que proporcionen niveles adecuados de protección de datos. Para ello, le entrega la atribución a la nueva Agencia para determinar los países que poseen niveles adecuados de protección, en base a 4 criterios: a) establecimiento de principios para el tratamiento de los datos personales; b) existencia de normas que reconozcan y garanticen los derechos de los titulares de datos; c) imposición de obligaciones de información y seguridad a los responsables del tratamiento de los datos, y d) determinación de responsabilidades en caso de infracciones.

Respecto de aquellos países que no califiquen como adecuados de protección de datos, el Proyecto del Ejecutivo autoriza la operación específica de transferencia de datos, bajo la condición de informar previamente y en forma electrónica a la Agencia, y solo en determinados 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 que pertenezcan a un mismo grupo empresarial, empresas relacionadas o sujetas a un mismo controlador de acuerdo a las normas de la ley 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

Propuesta:

- **Regulación base.** Como se señaló, esta materia sólo está regulada en el Proyecto del Ejecutivo. En esta materia, se sugiere mejorar la regulación de dicho proyecto.
- **Perfeccionamientos.** Se debe distinguir entre dos circunstancias:
  - **Países de nivel adecuado de protección.** Se sugiere que se eleve el estándar del proyecto de ley, de manera tal que la autoridad no se base simplemente en cuatro criterios cuya generalidad impide un grado mínimo de protección más allá de la determinación que efectúe la autoridad de control. En este sentido, se propone seguir el modelo del Reglamento Europeo, ya que una vez que entren en vigor las normas de protección de datos propuestas, nuestro país podrá situarse en la categoría de aquellos que cumplen con los estándares más altos, y en consecuencia, se podrá exigir a otros países obligaciones similares. En ese sentido, se propone incorporar como criterios los siguientes:

    a) El respeto de los derechos humanos y las libertades fundamentales; el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación; las normas sobre transferencias ulteriores de datos personales a otro tercer país; la jurisprudencia; así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos.

    b) La existencia y el funcionamiento efectivo de una o varias autoridades de control independientes, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos.

    c) Los compromisos internacionales asumidos por el tercer país de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales.

  - **Países sin nivel adecuado de protección pero con causal legal.** Para efectos de transferir los datos, es insuficiente que se exija una causal legal y sólo previo informe a la autoridad de control. En su lugar, se debería requerir legalmente de autorización previa a la autoridad de control y se debería contemplar estándares autónomos de revisión, que incluyan:

    a) Que se precise la finalidad del tratamiento de datos personales al momento de solicitar la autorización previa a la autoridad de control.

    b) Garantizar que se implementen las medidas de seguridad en los intercambios de información que se efectúen, incluyendo medidas y protocolos de seguridad que impidan tratamientos no autorizados por la ley, accesos no autorizados, pérdida, destrucción, adulteración, filtración o daños de los datos, que obliguen implementar las medidas de supervisión de las garantías de seguridad a nivel

interno, y que se registre los accesos o intercambios con los datos de identificación para efectos de trazabilidad de información.

c) Proteger expresamente los derechos de los niños, niñas y adolescentes, en este caso.

d) Fijar plazos máximos de almacenamiento de datos con fines de control fronterizo.

Propuesta de regulación de la transferencia internacional de datos personales
Transferencia internacional de datos personales a países con niveles adecuados de protección. 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 autoridad de control 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 existencia de uno más órganos o autoridades de control independientes encargado de la protección de datos a nivel nacional.* *d) La imposición de obligaciones de información y seguridad a los responsables y encargados del tratamiento de los datos.* *e) La determinación de responsabilidades en caso de infracciones.* *f) El Estado de derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas sobre transferencias ulteriores de datos personales a otro tercer país, la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos.* *g) Los compromisos internacionales asumidos por el estado u organismo internacional receptor de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales.* *La transferencia internacional de datos considera las operaciones de comunicación, transmisión o cesión de datos personales, según la necesidad y finalidades del tratamiento.*
Transferencia internacional de datos personales a países que no poseen niveles adecuados de protección. 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 solicitar la autorización previa y en forma electrónica a la autoridad de control para realizar la transferencia o transmisión internacional de datos.
El responsable deberá explicitar claramente la finalidad para la cual están siendo entregados los datos, al momento de su trasferencia.
Los datos transferidos sólo podrán ser susceptibles de tratamientos que sean conducentes a la finalidad descrita en el inciso anterior.
En el caso que la transferencia sea efectuada por un órgano del Estado, sólo podrá hacerse en el marco de sus atribuciones legales. Asimismo, el órgano sólo podrá entregar o intercambiar los datos que ha recolectado o almacenado en el ejercicio de sus propias competencias legales.
El responsable que transfiera datos personales a Estados extranjeros u organismos internacionales, deberán adoptar todas las medidas de seguridad que sean necesarias de acuerdo a la finalidad del tratamiento. Antes de efectuar la transferencia, el responsable que transfiere los datos deberá adoptar los protocolos de seguridad que impidan:

a) Tratamientos no autorizados por la ley;
b) Accesos por quienes no reúnan los perfiles autorizados para tratar los datos;
c) Pérdida, destrucción, adulteración, filtración o daños de los datos; y
d) Que permitan el registro de accesos o de intercambios con los datos de identificación de los usuarios, para efectos de trazabilidad de la información.

Tratándose de datos de niños, niñas y adolescentes, se deberán extremar las medidas de seguridad al momento de transferirlos a Estados extranjeros u organizaciones internacionales. Asimismo, los tratamientos de estos datos sólo pueden efectuarse atendiendo al interés superior de éstos y el respeto de su autonomía progresiva.
El responsable deberá procurar que los datos transferidos no sean almacenados más allá

de lo estrictamente necesario para cumplir los fines declarados en la autorización solicitada a la autoridad de control. Al momento de transferir los datos, el responsable deberá adoptar los protocolos que garanticen la destrucción de los mismos, una vez cumplida la finalidad declarada.

8. Autoridad de Control

Una de las graves deficiencias que adolece, desde su inicio, la regulación vigente sobre protección de datos personales fue la ausencia de una autoridad de control que tuviese competencias para que, en materia de tutela de datos personales, se capacite, recomiende, norme, fiscalice, resuelva casos y sancione los incumplimientos a la ley. Si bien nuestro país fue pionero en dictar una Ley de Protección de Datos Personales, en Latinoamérica, el resto de la región fue incorporando una autoridad de control ante la cual se pueda reclamar la protección de un derecho fundamental como es la autodeterminación informativa.

En el caso de la Moción, por carecer de iniciativa legislativa, no hay creación de una autoridad de control. La misma explicación de motivos del citado proyecto advierte que tal institución es clave para garantizar la protección de datos personales pero admite sus limitaciones en términos de competencias legislativas.

Por otro lado, el Proyecto del Ejecutivo crea una institución especializada y de carácter técnico, denominada "Agencia de Protección de Datos Personales", encargada de velar y fiscalizar el cumplimiento de esta normativa, que se relaciona con el Presidente de la República a través del Ministerio de Hacienda y se encuentra afecto al Sistema de Alta Dirección Pública. Es decir, se encontrará bajo la supervigilancia de una autoridad política, alejándose de los criterios indispensables de independencia y objetividad, que se requieren de un órgano de estas características.

Propuesta: Tratándose esta materia de uno de los aspectos más determinantes de las propuestas legislativas, resulta fundamental apuntar a los elementos que deben servir de base a la nueva institucionalidad. En ese sentido, se hace necesario establecer una autoridad de control verdaderamente independiente y de carácter colegiado, con el fin de superar el modelo de autoridad unipersonal y permitir que las decisiones sean discutidas y analizadas por más de un actor a fin de establecer los equilibrios necesarios.

En efecto, la independencia del ente garante es hoy un elemento central para lograr el estándar internacional de país adecuado fijado en el nuevo Reglamento Europeo. Lo anterior, se logra cumpliendo las siguientes exigencias:

- Autonomía del poder Ejecutivo para fiscalizar y sancionar adecuadamente el cumplimiento de las obligaciones de protección de datos personales en relación con la Administración del Estado y de privados.
- Evitar la asimetría de protección. El proyecto del Ejecutivo protege al ciudadano frente a privados pero no frente a los organismos públicos. En el primer caso se recurre a la Agencia de Protección de forma gratuita; en el segundo, debe recurrir directamente a las Cortes de Apelaciones, con los costos procesales que ello implica. Este diseño se explica por la falta de independencia.
- No se puede ser "juez y parte". La exigencia de independencia es una garantía para el ciudadano y los sujetos obligados –privados o públicos– y es una obligación de debido proceso.
- La separación de competencias entre el Consejo para la Transparencia y la Agencia de Protección de Datos personales generan los siguientes problemas de coordinación:

- **Se extreman los sesgos**. En función del "ego institucional", cada órgano tiende a extremar sus atribuciones, lo que genera necesariamente decisiones contrapuestas haciendo primar un derecho frente al otro.
- **Un tercero debe resolver la controversia.** Cuando los derechos se enfrenten, serán los tribunales los que deban resolver el conflicto. Se pierde la especialización de los órganos garantes y aumenta la posibilidad de fallos contradictorios.
- **Se elevan los costos para el ciudadano y se diluye su satisfacción final.** El sistema regulatorio se convierte en un sistema lento y, además, muy costoso, pues favorecerá la litigiosidad entre dos órganos públicos y los afectados deberán comparecer ante las Cortes.

Propuesta de autoridad de control
Autoridad de control: un único órgano garante. El Consejo para la Transparencia debería asumir las competencias de control en materia de transparencia y protección de datos personales. Dicha solución resuelve los problemas de independencia y autonomía, los costos de litigación para el usuario y de coordinación interagencial y conlleva los siguientes beneficios: a. ***Órgano especializado en la ponderación.*** *Estará obligado por mandato legal a resolver fundadamente los conflictos entre ambos derechos. Es un modelo más eficiente, es que el propio órgano resuelva en su seno la contienda y no se diluya la solución a los tribunales, lo que no obsta a que se revise la legalidad de sus decisiones ante las Cortes de Apelaciones.* b. ***Economías de escala.*** *Se aprovecha el conocimiento y experiencia del CPLT, en transparencia y protección de datos, así como toda su organización administrativa ya instalada.*

9. Infracciones y sanciones

Una de las grandes falencias de la Ley Nº 19.628 es la regulación vigente en materia de responsabilidad por infracciones a la ley. En ese orden de cosas, el artículo 23 establece sanciones de carácter indemnizatorio en el ámbito civil, en contra de la persona natural o jurídica u órgano público responsable de la base de datos, que cause un daño patrimonial o moral por un tratamiento indebido de los datos.

Al remitir a la justicia civil una infracción indeterminada, la ley actualmente vigente, transformó las obligaciones y deberes contenidos en ella en normas de difícil aplicación. Bajo la legislación vigente, el titular afectado por un tratamiento inadecuado de sus datos, debe contar con el patrocinio de abogado y someterse al procedimiento civil sumario, todo lo cual encarece y dilata indefinidamente la solución a un requerimiento que podría ser resuelto de manera precisa y eficaz, por un órgano garante independiente.

El Proyecto del Ejecutivo establece un régimen general de responsabilidad, estableciendo un catálogo de infracciones y dividiendo éstas en atención a su gravedad, en leves, graves y gravísimas. A su vez, fija un régimen de atenuantes de responsabilidad, un rango para las multas –que van de 1 a 5.000 UTM, que serán en definitiva determinadas por la Agencia– y un Registro Nacional de Cumplimiento de Sanciones.

La Moción, por su parte, también distingue las infracciones de acuerdo a su gravedad, en leves, graves y gravísimas, aunque en materia de multas dispone de un piso y un techo mayor, que comienza en 100 UTM y alcanzan las 10.000 UTM. La Moción también establece criterios para la determinación de las sanciones y entregando la atribución de aplicar las sanciones a los tribunales de justicia, esto como consecuencia de la imposibilidad constitucional que poseen los parlamentarios de entregar esta atribución a otro órgano que no posea las competencias para ello.

Propuesta:

- **Tipos de infracciones.** En general se sugiere seguir el listado del Proyecto del Ejecutivo, que es más detallado en el tipo de incumplimientos de la ley.
- **Sanciones.** Respecto de las sanciones, se debe distinguir.
    - En el caso del sector privado, el *quantum* de la sanción siempre puede ser discutido pero se requiere asegurar un mínimo de disuasión frente a infracciones futuras. Además, es relevante mantener como sanción principal –y no meramente accesoria– la inhabilitación perpetua de la base de datos infractora o la prohibición de desarrollar actividades de tratamiento de datos personales.
    - En el caso del sector público, se debe evitar que los incumplimientos queden sin sanción y se debe permitir un mayor arco de alternativas de castigo. En consecuencia, se podría ajustar la regla que comienza con la privación del 20% de la remuneración del jefe superior del servicio, para que vaya desde la censura hasta el 50% de la remuneración. Respecto de los datos sensibles, se recomienda reemplazar la sanción única de 50% de privación de la remuneración por un rango que puede empezar desde el 30 o 40 por ciento y alcance el 50 o 60 por ciento.

- **Registro Nacional de Cumplimiento y Sanciones.** Éste debería ser una obligación de transparencia activa de la autoridad de control.
- **Procedimiento sancionatorio.** Se sugiere no dividir funciones entre la autoridad de control y la Contraloría General de la República y concentrar toda la actividad sancionatoria en la Autoridad de Control. Para que ello sea posible, dicha autoridad debe satisfacer los estándares señalados en el punto 9.

Propuesta de infracciones y sanciones
Infracciones. 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. *Las infracciones a los principios y obligaciones establecidos en esta ley cometidas por los responsables y encargados 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 autoridad de control las comunicaciones previstas en esta ley o en sus reglamentos.* *e) No dar cumplimiento a las instrucciones impartidas por la autoridad de control 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 autoridad de control.
i) No efectuar las comunicaciones o no realizar los registros correspondientes en los casos de vulneración de las medidas de seguridad.
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 autoridad de control.

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.
Cuando concurran circunstancias atenuantes, la autoridad de control 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 autoridad de control podrá, además, exonerar la conducta del infractor. *En caso que exista reiteración o reincidencia, la autoridad de control 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.*
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 100 unidades tributarias mensuales.* *b) Las infracciones graves serán sancionadas con multa de 101 a 1.000 unidades tributarias mensuales.* *c) Las infracciones gravísimas serán sancionadas con multa de 1.001 a 10.000 unidades tributarias mensuales.* *La cuantía de la multa, dentro del rango asignado para cada tipo de infracción, será determinada por la autoridad de control 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 autoridad de control 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 autoridad de control podrá, además, exonerar la conducta del infractor.* *En caso que exista reiteración o reincidencia, la autoridad de control 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. *La autoridad de control podrá siempre, 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 autoridad de control 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.*
Sanciones en el caso de organismos públicos. 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 la presente ley. *Las infracciones a los principios y obligaciones establecidos en esta ley por parte del órgano público podrán consistir en censura y multa de hasta el cincuenta por ciento 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 40% al 60% de la remuneración mensual de la autoridad o jefe superior del órgano público y procederá la suspensión en el cargo de hasta treinta días.*
Registro nacional de sanciones. Créase el Registro Nacional de Cumplimiento y Sanciones administrado por la autoridad de control. El registro será público y su acceso gratuito. Dicha información deberá publicarse en el sitio web del organismo conforme a lo dispuesto por el título tercero de la Ley de Transparencia de la Función Pública y de Acceso a la Información de la Administración del Estado, aprobada por el artículo primero de la ley N° 20.285. *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.*

10. Entrada en vigencia y autorregulación

El éxito de una reforma de esta envergadura requiere de dos elementos que la garanticen: de un régimen de entrada en vigencia escalonado y diferenciado en términos de obligaciones en el tiempo y del reconocimiento expreso de mecanismos de autorregulación que sean eficaces.

Respecto de la entrada en vigencia, en el caso de la Moción, no cuenta con regla especial y, entonces, regiría una vez que se publique en el Diario Oficial. En el caso del Proyecto del Ejecutivo, tiene distintas reglas de vacancia legal. Para la entrada en vigencia de las modificaciones a la Ley N° 19.628, se dispone que rigen desde el primer día del 13° mes de publicada la ley en el Diario Oficial. Respecto del ajuste de las bases de datos elaboradas antes de la entrada en vigencia de la nueva ley, se dispone un plazo de 48 meses para ello, pero los titulares podrán ejercer sus derechos desde el primer día del mes 13° de publicada en el Diario Oficial. Los Reglamentos deberán dictarse dentro de los 6 meses de publicada la ley. La Agencia, en general, operará a partir de los 9 meses de publicada la ley, plazo en que el Presidente de la República deberá dictar los decretos con fuerza de ley para su planta y dotación de personal.

Por otro lado, se debe destacar los avances del derecho comparado en materia de autorregulación regulada, esto es, un mecanismo de auto-prevención de infracciones que contempla una supervisión y autorización oficial por parte de la Autoridad de Control y que genera incentivos al cumplimiento de las obligaciones de la ley. Si el mecanismo de autorregulación no se vincula directa y explícitamente con una atenuación de las sanciones, en caso de incumplimientos a la ley, entonces no alineará correctamente los incentivos al cumplimiento de las reglas de protección de datos personales.

Propuesta. Si bien dichos plazos siempre pueden ser revisados, se propone que se distingan otras reglas de entrada en vigencia, entre las que destacan:

- Diferenciación en la entrada en vigencia de la autoridad, de sus capacitaciones, del registro de las bases de datos, de certificación de los modelos de autorregulación y, finalmente, de las reglas de infracciones y sanciones.
- Establecer reglas de autorregulación que obliguen la certificación oficial por parte de la autoridad de control y que impliquen un incentivo para el cumplimiento de las obligaciones de la ley, al disponer una atenuación de la responsabilidad en caso de infracciones.

Propuesta de entrada en vigencia y autorregulación
Entrada en vigencia. *Artículo transitorio 1.- Facúltese al Presidente de la República para que, dentro del plazo de dieciocho meses contados 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) Determinar la fecha para la entrada en vigencia de las plantas que fije y la iniciación de actividades de la autoridad de control.* *2) Fijar la planta de personal de la autoridad de control 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. *2) Determinar la dotación máxima del personal de la autoridad de control.* *Artículo transitorio 2.- Dentro del plazo de un año, contado desde el inicio de las actividades de la autoridad de control, de conformidad al artículo precedente, el nuevo órgano deberá implementar un plan de capacitación dirigido hacia los responsables, encargados, intermediarios y organismos públicos en el tratamiento de datos, referido a los contenidos de la presente ley.* *Artículo transitorio 3.- Las disposiciones referidas al modelo de prevención de infracciones establecido en el artículo 54 y al cumplimiento de la obligación del responsable de llevar un registro de las actividades de tratamiento efectuadas bajo su responsabilidad, entraran en vigencia en el plazo de un dieciocho meses, contado desde la fecha de publicación de la presente ley en el Diario Oficial.* *En el mismo plazo, los responsables de tratamiento deberán registrar sus bases de datos ante la autoridad de control, en conformidad a lo dispuesto en esta ley.* *Artículo transitorio 4.- Las normas referidas a las infracciones y sanciones establecidas en el artículo XX y siguientes, entrarán en vigencia en el plazo de dos años contado desde la publicación de la presente ley en el Diario Oficial.*
Atenuante especial por prevención de infracciones. Las personas naturales o jurídicas que sean responsables del registro o base de datos personales o encargados de todo o parte del tratamiento de datos personales que incurrieren en alguna de las infracciones previstas en el artículo XX y siguientes, podrán atenuar su responsabilidad en la aplicación de las multas, si acreditan haber cumplido diligentemente sus deberes de dirección y supervisión para la protección de los datos personales bajo su responsabilidad o tratamiento. *Se considerará que los deberes de dirección y supervisión se han cumplido cuando, con anterioridad a la comisión de la infracción, los responsables del registro o base de datos personales o encargados del tratamiento de datos personales hubieren adoptado e implementado un modelo de organización, administración y supervisión para prevenir la infracción cometida, lo que deberá constar en un certificado emitido por la autoridad de control, conforme a lo dispuesto en el artículo siguiente.* *Estos certificados indicarán niveles de cumplimiento normativo de acuerdo a la clasificación que se determine reglamentariamente, los cuales deberán asociarse a los elementos que se señalan en el artículo siguiente.* *Modelo de prevención de infracciones. Para los efectos previstos en el artículo anterior, los responsables del registro o base de datos personales o encargados del tratamiento de datos personales podrán adoptar un modelo de prevención auto regulado que podrá contener, entre otros, los siguientes elementos:* *1) Designación de un encargado de prevención.* *2) Definición de medios y facultades del encargado de prevención. La Administración*

deberá proveer al encargado de prevención los medios y facultades suficientes para el desempeño de sus funciones, entre los que se considerarán, a lo menos:
a) Los recursos y medios materiales necesarios para realizar adecuadamente sus labores, en consideración al tamaño y capacidad económica del responsable del registro o base de datos personales o encargado del tratamiento de datos personales.
b) Acceso directo a la Administración para informarla oportunamente por un medio idóneo, de las medidas y planes implementados en el cumplimiento de su cometido y para rendir cuenta de su gestión y reportar a lo menos semestralmente.
3) Establecimiento de un sistema de prevención de las infracciones.
El encargado de prevención, en conjunto con la Administración, deberá establecer un sistema de prevención de las infracciones para el responsable del registro o base de datos personales o encargado del tratamiento de datos personales, que deberá contemplar, a lo menos, lo siguiente:
a) Considerando el estado de la técnica, el costo de la aplicación y su naturaleza, ámbito, contexto y fines del tratamiento, así como sus riesgos, su probabilidad y gravedad que implique para los derechos y libertades de las personas, se deberá previamente aplicar las medidas técnicas y organizativas, como la anonimización, a efectos de respetar los principios de protección de datos e integrar las garantías necesarias en el tratamiento. Asimismo, se deberán aplicar las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, sólo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. La protección pode defecto deberá alcanzar a la cantidad de datos personales recogidos, la extensión de su tratamiento, su plazo de conservación y a su accesibilidad.
b) 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 XX y siguientes.
c) 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.
d) La existencia de sanciones administrativas internas, así como de procedimientos de denuncia o persecución de responsabilidades pecuniarias en contra de las personas que incumplan el sistema de prevención de infracciones.
Estas obligaciones, prohibiciones y sanciones internas deberán señalarse en las propias regulaciones que los responsables del registro o base de datos personales o encargados del tratamiento de datos personales dicten al efecto y deberán comunicarse a todos sus colaboradores. Esta regulación interna deberá ser incorporada expresamente en los respectivos contratos de trabajo y de prestación de servicios de todos los trabajadores, empleados y prestadores de servicios de los responsables del registro o base de datos personales o encargados del tratamiento de datos personales, incluidos los máximos ejecutivos de la misma.
4) Supervisión y certificación del sistema de prevención de las infracciones.
a) El encargado de prevención, en conjunto con la Administración, deberá establecer métodos para la aplicación efectiva del modelo de prevención de las infracciones y su supervisión a fin de detectar y corregir sus fallas, así como actualizarlo de acuerdo al cambio de circunstancias de la respectiva entidad.
b) Los responsables del registro o base de datos personales o encargados del

tratamiento de datos personales podrán obtener la certificación de la adopción e implementación de su modelo de prevención de infracciones. En el certificado deberá especificar el nivel de cumplimiento de los requisitos establecidos en los numerales 1), 2) y 3) anteriores, en relación a la situación, tamaño, giro, nivel de ingresos y complejidad de la entidad.

5) Establecimiento de un sistema de arbitraje voluntario para el titular de datos personales.

a) Los responsables del registro o base de datos personales o encargados del tratamiento de datos personales deberán otorgar al titular de datos personales la alternativa de recurrir voluntariamente a un sistema de arbitraje voluntario, organizado por las entidades referidas, en forma exclusiva o conjunta, y gratuito para el titular señalado.

b) El sistema de arbitraje voluntario deberá tener requisitos de incorporación, inhabilidades y condiciones de ejercicio que garanticen su imparcialidad.

c) El árbitro que designe el titular de datos personales dentro de las personas que se han incorporado al sistema, deberá resolver las reclamaciones susceptibles de ejercer de acuerdo a esta ley.

d) Las decisiones del árbitro serán siempre voluntarias para el titular de datos personales, pero obligatorias para la entidad que corresponda si el titular de datos personales la acepta expresamente y renuncia a las demás acciones y derechos que le confiere la ley.

e) El plazo para resolver las reclamaciones será el que establezca el sistema de arbitraje, pero no podrá ser superior a 120 días.