Boletín N° 18.060-07

Proyecto de ley, iniciado en Moción de los Honorables Senadores señores Araya, Quintana y Saavedra, para perfeccionar la ley N° 21.719, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales, en los términos que indica.

1. Antecedentes generales

a. A través de la ley N° 19.628, del año 1999, sobre protección de la vida privada, se establecieron las normas que regulan el tratamiento y la protección de los datos de carácter personal de las personas naturales. La ley N° 19.628 constituyó un gran avance al momento de su dictación, siendo Chile el primer país latinoamericano en darse un marco regulatorio para el tratamiento y la protección de los datos personales. Sin embargo, progresivamente esta legislación fue perdiendo vigencia y eficacia, y pese a los varios esfuerzos legislativos realizados, ninguno de ellos dio fruto hasta el año 2017.

b. Así, durante el año 2017 los Honorables Senadores que integraban la Comisión de Constitución, Legislación, Justicia y Reglamento del Senado de la época, señores Harboe, Araya, De Urresti, Espina y Larraín, presentaron un proyecto de ley completo sobre protección de datos (Boletín N° 11.092-07).

c. En este contexto, y todo el proceso de debate técnico-político desarrollado, y haciéndose cargo del compromiso adquirido por el país en el marco del proceso de acceso de Chile a la OCDE, en el mes de marzo de este año 2017, el Gobierno de la Presidenta Bachelet - a través del Ministerio de Hacienda - presentó ante el Congreso Nacional, un proyecto de ley (Boletín N° 11.144-07) que regulaba la protección y el tratamiento de los datos personales y creaba la Agencia de Protección de Datos Personales.

d. Luego de una extensa tramitación legislativa, **el 13 de diciembre de 2024 se publica la ley N° 21.719, regula la protección y el tratamiento de los datos personales y crea la Agencia de Datos Personales.**

e. La ley N° 21.719 entra en vigencia el 1 de diciembre de 2026.

2. Principales orientaciones de política pública del proyecto de ley de datos personales

a. La primera orientación de política pública del proyecto de ley del año 2017, fue presentar una propuesta viable que permitiera avanzar en una nueva legislación orientada a perfeccionar y completar los vacíos de la normativa vigente, y que recogiera **los estándares internacionales contenidos en la legislación comparada y en las Directrices de la OCDE;** además de incorporar una autoridad de control, y un sistema institucional e incentivos que aseguraran la aplicación y cumplimiento de la ley. En definitiva, no se buscaba hacer un gesto testimonial, más bien, se promovió un proyecto que fuera atractivo y aprobable para los incumbentes.

b. Lo segundo, se buscó generar un texto que fuera el resultado de un proceso de análisis, diálogo y estudio técnico, en el que se balancearan y equilibraran las diferentes miradas y opciones técnicas, económicas, jurídicas y políticas que se promueven por los diversos actores, instituciones y grupos de interés que participan de este debate, alcanzando un marco regulatorio que proteja los derechos y libertades de las personas, garantice el tratamiento lícito de los datos personales por parte de terceros, sin entrabar ni entorpecer con ello la libre circulación de la información.

c. Por último, con el aporte y enriquecimiento del debate legislativo, se aspiraba a concluir con una **legislación moderna y flexible que cumpla los estándares internacionales, y deje al país en la vanguardia en materia regulatoria y permitiéndolo con seguridad y certeza — jurídica e institucional- enfrentar los desafíos del país de cara a los desafíos de la economía digital del siglo XXI.**

3.- Desarrollo de los objetivos del proyecto de ley

a. El proyecto de ley tuvo como **objetivo general** actualizar y modernizar el marco normativo e institucional con el propósito de establecer que el tratamiento de los datos personales de las personas naturales se realice con el consentimiento del titular o en los casos que autorice la ley, reforzando la idea que los datos personales deben estar bajo la esfera de control de su titular, favoreciendo su protección frente a toda intromisión de

terceros y estableciendo las condiciones regulatorias bajo las cuales los terceros, personas naturales o jurídicas, empresas y organizaciones públicas o privadas, pueden efectuar legítimamente el tratamiento de tales datos, asegurando estándares de calidad, información, transparencia y seguridad.

b. De esta forma, el **principal desafío regulatorio** era equilibrar la protección de los derechos y libertades de las personas que son titulares de los datos personales, especialmente el respeto y protección a la vida privada e intimidad, con la libre circulación de la información, asegurando que las reglas de autorización y uso que se establezcan no entraben ni entorpezcan el tratamiento lícito de los datos por parte de las personas, organismos y empresas.

c. Este desafío normativo implicaba dotar al país de una legislación moderna y flexible en materia de tratamiento de datos personales, que fuera consistente con los compromisos internacionales adquiridos luego de su incorporación a la OCDE y ajustada a las normas y estándares internacionales en la sociedad de la información.

4.- Fuentes normativas

a. Tal como se indicó en los antecedentes, la ley N°19.628 fue pionera en la región sobre regulación de los datos personales; Chile marcaba así un hito normativo y una orientación de política regulatoria: **el consentimiento, la ley, y las fuentes abiertas lícitas, como bases válidas y legítimas para el tratamiento lícito de datos, junto con la consagración de los derechos ARCO.**

b. La tecnología y el mundo fue evolucionando, y lo ha seguido haciendo hasta nuestros días, cada vez de manera más acelerada y vertiginosa; así, no **es extraño que la legislación vaya quedando rezagada en función de los cambios que se van sucediendo.**

c. Dentro de los cambios regulatorios más importantes que se provocó en el mundo fue la dictación por parte de la Unión Europea del **Reglamento General de Protección de Datos, del año 2016,** el cual entró en vigencia el 25 de mayo de 2018. Este nuevo orden normativo vino a regular todo un mundo surgido a partir de internet y las plataformas

digitales. Estos nuevos estándares implicaron un gran cambio para los buscadores y la definición de nuevos centros de responsabilidad.

d. Durante el proceso de elaboración del proyecto de ley, el Reglamento de la UE ya estaba aprobado, aunque no vigente, por lo que **fue una fuente que inspiró varias reglas del proyecto del Ejecutivo;** durante su tramitación legislativa entró en vigencia este Reglamento, y el país se encontraba renegociando los términos de su acuerdo comercial con la UE; lo anterior hacía aconsejable cuidar o tener presente estas reglas durante ese proceso de negociación.

e. En este contexto, una parte importante de los legisladores, y también del Ejecutivo, creyó que, en razón del acuerdo con la Unión Europea, Chile debía ajustarse al Reglamento de Protección de Datos de la UE y así, ser considerado un país "adecuado" en materia de privacidad y protección de datos personales. Lamentablemente, como ocurre en algunas oportunidades, **no se recurrió a las fuentes para indagar cuales eran las exigencias especificas del Acuerdo.**

f. En efecto, el **Acuerdo Marco Avanzado (AMA) entre Chile y la Unión Europea** tuvo un cierre técnico en octubre de 2021 y un cierre político en diciembre de 2022. Finalmente, Chile y la Unión Europea firmaron el Acuerdo el 13 de diciembre 2023, en Bruselas, y la entrada en vigor se espera para cuando las partes completen los respectivos procedimientos legislativos y administrativos, tanto en la UE y sus estados miembros como en el Congreso Nacional establece lo siguiente:[1]

CAPÍTULO 26

COMERCIO DIGITAL

SECCIÓN A

DISPOSICIONES GENERALES

ARTÍCULO 26.3

Derecho a regular

[1] https://www.subrei.gob.cl/acuerdos-comerciales/modernizacion-ue-chile

Las Partes reafirman ***el derecho a regular dentro de sus territorios para lograr objetivos legítimos de políticas****, como la protección de la salud pública, los servicios sociales, la educación, la seguridad, el medio ambiente (incluido el cambio climático), la moral pública, la protección social o de los consumidores,* ***la privacidad y la protección de datos*** *o la promoción y la protección de la diversidad cultural.*

SECCIÓN B
FLUJOS DE DATOS Y PROTECCIÓN DE DATOS PERSONALES

ARTÍCULO 26.5
Flujos de datos transfronterizos

Las Partes se comprometen a garantizar los flujos de datos transfronterizos para facilitar el comercio digital. Para tal fin, una Parte no restringirá los flujos de datos transfronterizos entre las Partes:

a. *exigiendo el uso de instalaciones informáticas o elementos de red en su territorio para el tratamiento, incluso mediante la imposición del uso de instalaciones informáticas o elementos de red que están certificados o aprobados en el territorio de una Parte;*

b. *exigiendo la localización de datos en su territorio para su almacenamiento o tratamiento;*

c. *prohibiendo el almacenamiento o el tratamiento en el territorio de la otra Parte;*

d ni, supeditando la transferencia de datos transfronteriza al uso de instalaciones informáticas o elementos de red en su territorio o a requisitos de localización en su territorio.

ARTÍCULO 26.6
Protección de los datos personales y de la privacidad

1. ***Cada Parte reconoce que la protección de los datos personales y de la***

privacidad es un derecho fundamental y que los altos estándares a este respecto contribuyen a la confianza en la economía digital y al desarrollo del comercio.

2. ***Cada Parte podrá adoptar o mantener las medidas que considere adecuadas para garantizar la protección de los datos personales y de la privacidad, incluida la adopción y aplicación de normas para la transferencia transfronteriza de datos personales***. *Nada de lo dispuesto en esta parte del presente Acuerdo afectará a la protección de los datos personales y de la privacidad garantizada por las medidas de una Parte*.

g. Como puede observarse, **el Acuerdo con la UE establece la obligación reciproca de las Partes de garantizar la privacidad y protección de los datos personales,** y al mismo tiempo, **deben garantizar los flujos de datos transfronterizos con el fin de facilitar el comercio digital.** Para este propósito, **ninguna de las Partes debe restringir los flujos de datos transfronterizos.**

h. Ahora bien, **Chile es un país abierto al mundo,** y sus principales socios tecnológicos son Estados Unidos, China, otros países del Asia Pacifico, y en menor medida, la Unión Europea.

i. La legislación de Estados Unidos no tiene reglas especiales sobre protección de los datos personales (a nivel federal) así, **la protección de la privacidad y de los datos personales deriva de precedentes jurisprudenciales constituidos en base al derecho a la privacidad** (contenido en varias enmiendas como inmunidades frente a injerencias del Estado o de terceros). Las protecciones o indemnidades jurídicas en materia de protección de la información personal han sido desarrolladas a partir de la consagración de los derechos de los consumidores. La tutela de estos derechos se otorga en sede judicial, no existiendo un órgano de control de carácter administrativo.

j. **Estados Unidos y las empresas tecnológicas de ese país son particularmente resistentes a legislaciones muy restrictivas en materias de desarrollos tecnológicos, especialmente de cara a la sociedad de la información y la economía digital.** Sus

posiciones - las de EE UU- se expresan con energía en los foros internacionales. En la OCDE, Estados Unidos ha hecho ver en más de una oportunidad sus comentarios y observaciones respecto de algunas de las orientaciones del proyecto de ley que se tramitaba en Chile sobre datos personales.

k. El flujo de datos - en el mundo de hoy- es esencialmente transfronterizo, las eventuales ventajas competitivas que pueda tener Chile en la economía digital dicen relación con su **capital humano,** pero también, **con un marco jurídico moderno, equilibrado y coherente, y particularmente flexible con aquellos sistemas normativos con los cuales le corresponda interactuar.**

l. Por otro lado, pasaron más de siete años desde el ingreso del proyecto de ley hasta su aprobación final. En este período el mundo ha cambiado vertiginosamente en materia de desarrollo tecnológico y de la información. Algunos de los principales cambios son los siguientes:

- *La multiplicación de las redes sociales (X, Facebook, Instagram, Tik Tok, Wsp, Pinterest, Linkedln, Youtube, Snapchat, entre otras).*
- *La incorporación de China como desarrollador de aplicaciones masivas (al 2024 la plataforma Tik Tok superó los 1.500 millones de usuarios mensuales activos a nivel mundial).*
- *La creciente injerencia política de las redes sociales en los procesos electorales a través de la difusión de noticias falsas (a través de milicias digitales).*
- *Big data y analítica predictiva.*
- *Criptoeconomía y block chain.*
- *Inteligencia artificial y machine learning.*

m. Muchos o casi todos los cambios expuestos anteriormente **impactan en el manejo y gestión de la información de las personas.** Un número importante de las reglas que conocemos y discutimos durante la tramitación de la ley de datos personales quedan superadas por algunos de estos desarrollos tecnológicos. **La ciencia y la tecnología evolucionan más rápido que el Derecho.**

n. Ahora bien, **el mayor desafío que actualmente enfrenta la humanidad es definir los propósitos, los fines, los bordes (límites) y la gobernanza de la inteligencia artificial.**

o. La presente propuesta legislativa **no tiene como finalidad regular estos nuevos escenarios tecnológicos y los desafíos que nos presenta.** El Ministerio de Ciencia tiene mucho que hacer y decir en este ámbito. El Derecho es absolutamente insuficiente y refractario para enfrentar estos nuevos desafíos regulatorios.

p. Cabe tener presente, que en la actualidad la Unión Europea se encuentra revisando su legislación en materia de datos personales. En efecto, la Comisión Europea presentó en noviembre de 2025 un paquete normativo denominado ***Digital Omnibus***,[2] con el que propone modificar el **Reglamento General de Protección de Datos (GDPR)** y otras normas digitales de la Unión Europea.

q. Entre los cambios propuestos se encuentran los siguientes: redefinir qué se considera "dato personal" —por ejemplo, permitir que datos seudonimizados no entren en la categoría de datos personales si no pueden asociarse razonablemente a una persona concreta—; flexibilizar las obligaciones para empresas pequeñas y medianas (menos registro de actividades de tratamiento, exenciones si no hay riesgos elevados); y **facilitar que empresas de IA usen datos personales como base legítima para entrenamiento de modelos sin consentimiento explícito.**

r. Además, el paquete normativo propuesto busca simplificar reglas sobre cookies, reporte de incidentes, interoperabilidad de datos, y extender los plazos para cumplimiento de regulaciones complejas —por ejemplo, posponer obligaciones estrictas sobre IA de "alto riesgo".

s. La Unión Europea progresivamente ha ido perdiendo competitividad en materia de desarrollo tecnológico. El informe Draghi de 2024 atribuye el déficit de competitividad de la UE, en parte, **a las cargas administrativas y a las inconsistencias regulatorias.** En concreto, el informe señala que el entorno regulatorio impone demasiadas restricciones a la innovación, especialmente en el sector digital, y obstaculiza el

[2] https://digital-strategy.ec.europa.eu/en/policies/digital-rulebook

crecimiento de las startups europeas Para el mandato 2024-2029, la Comisión se comprometió a abordar las fallas identificadas en el informe Draghi y emprendió un esfuerzo de simplificación. El resultado de este trabajo es en parte la desregulación propuesta.

t. Como puede observarse **Chile avanza en un sentido contrario al mundo desarrollado:** mientras Europa y Estados Unidos avanzan en la simplificación regulatoria, Chile se encuentra inmerso en el proceso de implementación de la ley N° 21.719, que elevó el estándar normativo al Reglamento de la UE de 2016 (GDPR) de 2016), que es abandonado por Europa.

u. Una última consideración que le pone **sentido de urgencia** a varias de estas enmiendas se vincula con los efectos de la compleja **política comercial del actual gobierno de Estados Unidos.** Si bien Chile tiene un tratado de libre comercio con ese país, no quedó excluido de los aranceles generales que fueron fijado en un 10%.

v. Con posterioridad a esta decisión de EE.UU. se abrió un espacio de negociación. Así, el pasado **16 de abril de 2025, la subsecretaria de Relaciones Económicas Internacionales (Subrei) de Chile, encabezó una reunión con el representante comercial de Estados Unidos** (USTR, por sus siglas en inglés). Como resultado de ese encuentro, se logró agendar reuniones de trabajo con el objeto de avanzar en el fortalecimiento de la relación económica-comercial bilateral entre ambos países, de acuerdo con lo establecido en el Acuerdo de Libre Comercio vigente desde 2004. Las materias que se abordarán en estos encuentros serán las siguientes:[3]
   - Economía digital.
   - Seguridad económica (inversiones y permisología).
   - Barreras no arancelarias.

w. En términos más concretos, según el informe "National Trade Estimate" del USTR las principales preocupaciones de Estados Unidos, serían las siguientes:
   - **Propiedad intelectual:** EE.UU. considera que Chile no está cumpliendo

[3] https://www.subrei.gob.cl/sala-de-prensa/noticias/detalle-noticias/2025/04/16/subsecretaria-claudia-sanhueza-lidera-reuni%C3%B3n-con-representante-comercial-de-estados-unidos

adecuadamente ciertas obligaciones del TLC, como la ratificación del Acta de UPOV 1991. También existe preocupación por la efectividad del sistema chileno frente a la piratería digital y satelital, así como la responsabilidad de los proveedores de servicios de internet.

- **Sector farmacéutico:** Hay inquietudes sobre la rapidez y eficiencia del sistema chileno para resolver disputas de patentes, así como la protección de los datos comerciales no publicados relacionados con la aprobación de medicamentos.
- **Tratamiento de datos digitales:** El USTR advierte sobre la falta de claridad en directrices sobre cláusulas contractuales y definiciones clave que generan incertidumbre en empresas que realizan transferencias internacionales de datos. También existe preocupación por las reglas sobre extraterritorialidad de la ley.
- **Sistema de pensiones:** EE.UU. observó con preocupación que la reforma incluya la subastas o licitación de stock (clientes antiguos de la AFP).

x. Considerando que la nueva ley de datos personales entra en vigencia en diciembre de 2026, este nuevo marco regulatorio sobre la protección de datos puede ser un elemento relevante (aunque no sea el foco principal declarado) en la agenda de comercio digital, inversiones y confianza regulatoria que se discute entre Chile y EE.UU. Una regulación clara y alineada con estándares internacionales puede mejorar la posición de Chile frente a las preocupaciones de EE.UU. sobre flujos de datos, barreras digitales y otras.

y. En particular, las principales preocupaciones de EE.UU frente a la nueva ley de datos:

- **Restricciones en las transferencias transfronterizas de datos.** El USTR considera las restricciones a la libre circulación de datos—como requisitos de localización de datos o condiciones excesivas para su transferencia internacional—como barreras al comercio digital.
- **Exigencia de representación local para proveedores extranjeros.** Bajo la nueva ley, proveedores de servicios fuera de Chile deben designar y mantener un representante domiciliado en Chile para efectos de notificaciones y acceso por parte del regulador. El USTR considera que estas exigencias pueden aumentar costos y complejidad operativa, generando incertidumbre para empresas.
- **Alto nivel de sanciones y régimen punitivo.** La ley chilena establece multas

elevadas: hasta 20 000 UTM (~USD 1,5 millones) por infracciones muy graves, con posibilidad de multas adicionales o equivalentes al porcentaje de ingresos de la empresa. Desde la perspectiva del USTR, esto puede verse como un riego regulatario excesivo, especialmente si se impone sin una claridad suficiente en su aplicación o criterios diferenciados según tamaño o naturaleza de empresa.

- **Ambigüedad en definiciones y alcance (incluidas las de "datos sensibles").** El USTR presiona porque las regulaciones de protección de datos no sean ambiguas ni abrumen a las empresas con términos confusos. Chile amplió las categorías de datos considerados "sensibles": desde datos biométricos hasta ideológicos o de condiciones socioeconómicas. Sin una delimitación clara, esto podría generar incertidumbre sobre qué cae bajo regulaciones estrictas.

z. Hasta ahora, en las negociaciones arancelarias, aunque los temas principales siguen siendo los bienes y los aranceles, los aspectos de economía digital (incluyendo datos) pueden emerger como parte de la "agenda moderna" de comercio, de la cual EE.UU. puede exigir avances o garantías.

aa. **El país no puede estar obligado o presionado a legislar o modificar** su **legislación en base a presiones u observaciones de países o economías externas, pero tampoco puede desatender esas observaciones si tienen algún grado de razonabilidad**

bb. El balance que arrojó como resultado el texto final de la ley de protección de datos personales, luego de su extensa tramitación, **no es adecuado. No se alcanzó un texto equilibrado. No se compatibilizó racionalmente la protección de los datos personales, con la libre circulación de la información, y el derecho de las personas - soberanía personal- para decidir sobre el uso personal de su información.**

5 .- Objetivo del proyecto de ley

El presente proyecto de ley tiene por objeto modificar la ley N°21.719, regula la protección y el tratamiento de los datos personales y crea la Agencia de Datos Personales, a efecto de corregir o enmendar aquellas normas que claramente desbalancearon la ley de datos personales (entre la protección del titular y la libre circulación de la información), las que generaron algunos resultados indeseados,

aquellas reglas que están, incluso fuera de la línea de las mismas reglas de la UE; y por último, las normas que resultan muy difícil de implementar o son claramente impracticables.

6 .- Reformas propuestas y fundamento

a. ***Se limita el ámbito de aplica de la ley y se consagra la extraterritorialidad de la ley chilena***

El inciso segundo del **artículo 1 de la nueva ley de protección de datos personales contenida en la ley N°21.719** consagra la regla de aplicación material, personal y territorial de la ley, al establecer lo siguiente:

> *"Todo tratamiento de datos personales que realice una persona natural o Jurídica, incluidos los órganos públicos, debe respetar los derechos y libertades de las personas y quedará sujeto a las disposiciones de esta ley. ".*

El **artículo 1 bis** de la misma ley describe hipótesis que están cubiertas con la regla general enunciada en la regla general del artículo 1. Su incorporación es una mala decisión de técnica legislativa, ya que al hacer un listado cerrado la ley solo será aplicable a las hipótesis ahí descritas. En un ámbito en que la deslocalización y los cambios tecnológicos son casi imposibles de prever, **petrificar la regla que determina el espacio o ámbito de validez** de **la ley** es, en la más convencional de las calificaciones, inconveniente.

Por otro lado, el **artículo 1 bis** de la misma ley, contiene una **regla de extraterritorialidad de la ley,** al establecer que, independiente de dónde esté localizada una empresa o compañía, si un residente en Chile realiza operaciones en una plataforma, esa operación quedará sujeta a la ley chilena. Esta regla impone un gravamen a las empresas tecnológicas que no parece razonable, muchas de ellas son empresas localizadas en EEUU, y por ello resultará muy complejo materializar esta norma. Adicionalmente, se produce una evidente contradicción entre las dos reglas expuestas.

El conjunto de reglas que contenía el proyecto de ley original, aprobadas en el primer

trámite constitucional por el Senador, resolvía razonablemente la regulación de los tratamientos de datos transfronterizos, no de manera ingenua, más bien, de manera realista.

b. ***Ampliación del concepto de dato personal sensible a condiciones o circunstancias irrisorias***

La ley N°21.719 establece con relación a los datos sensibles lo siguiente:

> ***"Datos personales sensibles: tendrán esta condición aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad****, que revelen el origen étnico o racial,* ***la afiliación política****, sindical* ***o gremial, la situación socioeconómica****, las convicciones ideológicas o filosóficas, las creencias religiosas, los datos relativos a la salud, al perfil biológico humano, los datos biométricos, y la información relativa a la vida sexual, a la orientación sexual y a la identidad de género de una persona natural. ".*

El Reglamento de la UE al referirse a los "datos sensibles" o "datos que requieren una especial protección", señala lo siguiente: *"datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física.*

Con la incorporación de categorías tan genéricas y ambiguas como los ***"datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad''***, se está incorporando TODA característica o condición de una persona, como el color de pelo, de ojos, la altura, el peso, la edad, etc. Las características morales de las personas son imprecisables y totalmente subjetivas.

- ¿Qué puede tener de sensible una característica o un dato como cualquiera de los anteriores?

- ¿Por qué ese tipo de información requerirían una protección reforzada?

Las mismas preguntas surgen con la protección a datos que son públicos: *afiliación política, situación socioeconómica y afiliación gremial* ¿Qué discriminación o lesión de derechos se busca proteger para requerir una protección especial de esta información?

c. ***Regulación de las fuentes de acceso público***

En segundo término, la ley define como lo siguiente:

> ***"Fuentes de acceso público****: todas aquellas bases de datos o conjuntos de datos personales, cuyo acceso o consulta puede ser efectuada en forma lícita por cualquier persona, tales como el Diario Oficial, medios de comunicación o los registros públicos que disponga la ley. El tratamiento de datos personales provenientes de fuentes de acceso público se someterá a las disposiciones de esta ley.".*

Las fuentes de acceso público son de las más importantes bases de legitimidad para el tratamiento de datos personales, de ahí que su regulación es clave en un sistema moderno de gestión de datos y en la economía digital.

El proyecto de ley aprobado originalmente (Mensaje del Ejecutivo) establecía lo siguiente:

> ***"Fuentes de acceso público****: todas aquellas bases de datos o conjuntos de datos personales, públicos o privados, cuyo acceso o consulta puede ser efectuada en forma lícita por cualquier persona, tales como el Diario Oficial, medios de comunicación o los registros públicos que disponga la ley, siempre que no existan restricciones o impedimentos legales para su acceso o utilización.*
>
> *Las dudas o controversias que se susciten sobre si una determinada base de datos es considerada fuente de acceso público serán resueltas por la Agencia de Protección de Datos Personales, quien podrá identificar categorías genéricas, clases o tipos de registros o bases de datos que posean esta condición.".*

Existe una brecha significativa entre la regla propuesta y la aprobada, sin que mediara una justificación técnica que sustentara esta modificación.

Sin embargo, el punto más complejo en esta materia es la supresión de las fuentes de acceso público como base de licitud del tratamiento de datos personales. En efecto, la regla del artículo 13 contiene las fuentes de licitud del tratamiento de datos, sin consentimiento del titular. La redacción original incluía en su letra a) lo siguiente:

> *Artículo 13.* ***Otras fuentes de licitud del tratamiento de datos****. Es lícito el tratamiento de datos personales, sin el consentimiento del titular, en los siguientes casos:*
>
> *a) Cuando los datos han sido recolectados de una fuente de acceso público y su tratamiento esté relacionado con los fines para los cuales fueron entregados o recogidos.*

En la redacción actual del artículo 13, esta letra fue suprimida. Por lo tanto, para tratar datos contenidos en fuentes de acceso público se requerirá del consentimiento del titular.

Frenar el tratamiento de los datos provenientes de fuentes de acceso público originará múltiples controversias y no existen razones técnicas que justifiquen esa decisión

d. ***Regulación de los derechos de supresión o cancelación y oposición***.

A través de los artículos 7 y 8 se regulan los **derechos de supresión y oposición.** Es evidente que se trató de hacer un esfuerzo de simplificación de estas reglas, lo que siempre es valorable; sin embargo, el resultado es confuso, y como resultado de esta simplificación se eliminaron y mezclaron varias de las hipótesis, dejando una regulación parcial e insuficiente.

Asimismo, en el segundo trámite, que fue recogido en el texto final de la ley, se suprimió el artículo 8° bis, que establecía el **derecho de oposición a valoraciones personales automatizadas.**

Este conjunto de enmiendas dejó un sistema de derechos ARCO poco consistente que

requiere una revisión para darle coherencia y racionalidad.

e. ***Se crea el derecho a bloqueo***.

Cuando un titular deduce una reclamación, y resulta procedente, puede solicitar la suspensión o bloqueo del tratamiento de los datos que le conciernen, en tanto se resuelve la reclamación Se trata de una medida procesal. Esta acción procesal tiene un carácter cautelar y provisorio, y en ningún caso puede ser considerado un "derecho autónomo" como los derechos ARCO (así lo hace el proyecto),

Sin embargo, se incorpora un artículo 8 ter que introduce una regulación relativa al derecho a bloqueo como un "derecho subjetivo autónomo", esto es, el titular de datos puede deducir el bloque sin necesidad de ejercer una acción principal. Este modelo rompe la armonía de nuestro sistema normativo donde las acciones cautelares están subordinadas o son complementarias a la acción de fondo o sustantiva.

Ahora bien, la regla propuesta en el artículo 8° ter se asemeja al "derecho a la limitación del tratamiento" que se consagra en el artículo 18 del Reglamento de la UE. Este derecho autoriza al interesado a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones que se establecen, Como puede observarse, este derecho en nada se vincula con el bloqueo temporal que contempla nuestro régimen normativo.

Adicionalmente, **no es razonable, prudente, ni necesario, exportar todos los institutos jurídicos de un modelo normativo a otro; ciertamente el reglamento europeo es una referencia mundial en materia de legislación sobre datos personales, pero de ahí no se sigue que haya que "copiar" todas sus reglas.**

f. ***Obligaciones para los responsables de datos domiciliados en el extranjero***

Se establece en el artículo 10 inciso segundo la obligación de constituir un domicilio y un representante en Chile para las empresas o instituciones extranjeras, y acreditarlos ante la Agencia. Considerando la velocidad con que circula la información en la red, el caudal de datos personales que se movilizan, las redes sociales, los flujos comerciales,

los intercambios financieros, la deslocalización de los servicios, entre otros fenómenos; pretender que esas compañías cumplan esta obligación es simplemente carecer de juicio de realidad

Recientemente se produjo una controversia en Brasil con la red social X de propiedad de Elon Musk. Ei Tribunal Supremo Federal de Brasil suspendió las operaciones de la red social hasta que dicha empresa no acreditara un representante legal en Brasil, y cumpliera con el bloqueo de cuentas de usuarios que fueron condenados por propagar noticias falsas, principalmente en el contexto de las campañas electorales. Finalmente, la empresa cumplió la obligación impuesta por la justicia.

Ambas situaciones podrían considerarse simétricas, la regla legal y la resolución judicial; sin embargo, no es así. La diferencia no está en el contenido material de la obligación o su pertinencia, lo que hace que ambos casos sean distintos es el tamaño de mercado de cada uno de estos países, y consecuentemente, su poder negociador.

Ahora bien, tampoco es razonable que el responsable de datos que no tenga domicilio en Chile carezca de toda forma de contacto o vinculación con los titulares de datos que residan en Chile, como tampoco que quede completamente excluido del perímetro regulatorio de la Agencia. Esta exigencia, razonable, queda bien resuelta con lo dispuesto en el inciso segundo del artículo 14 de la ley, que señala lo siguiente:

> *"El responsable de datos que no tenga domicilio en Chile y que realice tratamiento de datos de personas que residan en el territorio nacional, deberá señalar y mantener actualizado y operativo, un correo electrónico u otro medio de contacto idóneo para recibir comunicaciones de los titulares de datos y de la Agencia.".*

g. ***Reducción de las causales que autorizan la transferencia de datos***.

El artículo 27 establece las reglas de autorización para la transferencia internacional de datos personales, tanto generales como específicas. El proyecto de ley original y el texto aprobado en el primer trámite incluía una hipótesis que finalmente no fue recogida en el texto final, cuya omisión representa un grave entorpecimiento del comercio

internacional, de la economía digital y la gestión de servicios globales.

En efecto, se trata de la transferencia de datos entre sociedades o entidades que pertenezcan a un mismo grupo empresarial, empresas relacionadas o sujetas a un mismo controlador en los términos previstos en la Ley de Mercado de Valores.

h. ***Régimen especial de tratamiento de datos relativos al sistema de enjuiciamiento penal***.

El Titulo IV de la ley denominado "Del tratamiento de datos personales por los órganos públicos", establece las normas bajo las cuales los órganos de la administración del Estado pueden realizar tratamiento de datos, incluyendo los regímenes especiales que se regulan en el artículo 24. Particularmente, la letra a) regula el tratamiento de datos personales relativos al sistema de enjuiciamiento penal Las siguientes letras de este mismo artículo consagran otras hipótesis, también sujetas a este régimen especial de regulación. En general se trata de ámbitos sensibles en donde el Estado requiere mayores espacios de libertad para desplegar su acción en virtud del interés colectivo. No obstante lo anterior, los órganos del Estado quedan sujeto algunas restricciones vinculadas con los derechos fundamentales de las personas y los principios y deberes generales del Estado.

Dentro de los datos personales que trata el Estado, los datos relativos a infracciones penales, civiles, administrativas y disciplinarias, requieren una especial atención. Así mismo, de este conjunto de información personal, las reglas relativas a sanciones penales son datos que, además, requieren una protección especial. El artículo 25 contiene la regulación específica para este tipo de datos, incluyendo la obligación de secreto y las prohibiciones de tratamiento.

Pues bien, la letra a) del artículo 24 señala lo siguiente:

> *"a) Aquellos que se realicen confines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas las actividades de protección y prevención frente a las amenazas y riesgos contra la seguridad pública, protección a víctimas y testigos, análisis criminal y reportabilidad de la información criminal.* ***Respecto de los datos que***

se realicen con esta finalidad, no será aplicable lo dispuesto en el artículo 25.*"*.

Descontadas las reiteraciones y redundancias de la redacción aprobada, la norma excluye el tratamiento de estos datos de la regla del artículo 25, norma dictada expresamente para regular estos tratamientos. Este agregado es una contradicción con el modelo regulatorio y deja sin sentido al artículo 25; y aún más, elimina todo estándar de prudencia y cuidado en el tratamiento de datos tan "sensibles" o "delicados" como los datos relativos a sanciones penales.

i. ***Desproporción de las sanciones***.

Una ley que no contenga un sistema de control, fiscalización y cumplimiento bien diseñado, es **letra muerta;** uno de los elementos centrales del sistema de control es contar con un **régimen sancionatorio equilibrado,** esto es, **infracciones bien tipificadas y multas proporcionales a la infracción** El proyecto de ley presentado por el Ejecutivo definió infracciones leves con sanciones de amonestación escrita o multa de 1 a 50 unidades tributarias mensuales (UTM); infracciones graves con multa de 51 a 500 UTM; infracciones gravísimas con multa de 501 a 5.000 UTM. Posteriormente, el Senado elevó las multas: infracciones leves con amonestación o multa de 1 a 100 UTM; infracciones graves con multa de 101 a 5.000 UTM, e infracciones gravísimas con multa de 5.001 a 10.000 UTM. Finalmente, la Cámara de Diputados elevó el monto de las multas El resultado final es el siguiente:

a) *Las **infracciones leves** serán sancionadas con amonestación escrita o multa de hasta **5.000 unidades tributarias mensuales**.*
b) *Las **infracciones graves** serán sancionadas con multa de hasta **10.000 unidades tributarias mensuales**.*
c) *Las **infracciones gravísimas** serán sancionadas con multa de hasta **20.000 unidades tributarias mensuales**.*

En el artículo 35 no conforme con establecer estas multas fuera de toda razonabilidad, incorporó lo siguiente:

"<u>En cada caso,</u> la Agencia señalará las medidas tendientes a subsanar

las causales que dieron motivo a la sanción, las que deberán ser adoptadas en un plazo no mayor a sesenta días, de lo contrario se impondrá ***un recargo de 50% a la multa cursada****, sin perjuicio de lo establecido en el artículo 49.*

En caso de que exista reincidencia, de conformidad al literal a) del inciso segundo del artículo 36, la Agencia podrá ***aplicar una multa de hasta tres veces el monto asignado a la infracción cometida****.*

En caso de que el infractor corresponda a una empresa distinta de aquéllas definidas como empresas de menor tamaño en el artículo segundo de la ley N° 20.416, que reincida en infracción de carácter grave o gravísima en los términos del literal a) del inciso segundo del artículo 36, ***la multa podrá alcanzar a la más gravosa entre la señalada en el inciso anterior o hasta el monto correspondiente al 2% o 4% de los ingresos anuales por ventas y servicios y otras actividades del giro en el último año calendario, según se trate de infracciones graves o gravísimas, respectivamente****. ".*

Dejando a un lado la pobreza del lenguaje (tres párrafos seguidos se encabezan con la misma frase), cada regla es peor que la otra. Al construir esta norma parece que no hubo conciencia alguna de lo que significaba cada una de ellas, el monto que podría implicar cada una de esas sanciones, y la proporción que existía entre el monto de la sanción y la infracción.

En un mundo en que el tráfico de datos es una realidad, donde las vulneraciones de los sistemas también son una realidad, el foco de la política pública debería estar en la prevención, la educación digital, disponer de mecanismos eficientes para controlar desviaciones o filtraciones de información, pero concentrase en una acción punitiva, en una Agencia Policial, carece de toda racionalidad. Ninguna de estas multas se terminará cursando ni cobrando, simplemente porque son desproporcionadas e irracionales.

j. ***Falta de coordinación en la estructura del texto***

El proyecto de ley tenía una secuencia lógica, contenía un Título séptimo dedicado a la regulación del sistema infraccional y de cumplimiento, integrado por seis párrafos que

abordaban el régimen sancionatorio, recursivo, de responsabilidad, y una cuestión central para el diseño normativo propuesto: el modelo de cumplimiento. Así, el esquema era el siguiente:

Título VII De las infracciones y sus sanciones, de los procedimientos y de las responsabilidades

- *El Párrafo Primero "De la responsabilidad, las infracciones y las sanciones aplicables a las personas naturales o jurídicas de derecho privado".*
- *El Párrafo Segundo "De los procedimientos administrativos".*
- *El Párrafo Tercero "Del procedimiento de reclamación judicial".*
- *El párrafo Cuarto "De la responsabilidad de los órganos públicos, de la autoridad o jefe superior del órgano y de sus funcionarios".*
- *El párrafo Quinto "De la responsabilidad civil".*
- *El Párrafo Sexto Del modelo de prevención de infracciones".*

Pues bien, en una "extraña" curiosidad, fue eliminado el Párrafo Sexto, y solo se contempla hasta el Párrafo Quinto "De la responsabilidad civil" que parte en el artículo 47 y termina en el 53, y solo el 47 se refiere a la responsabilidad civil, todos los demás artículos están referidos al modelo de cumplimiento Este parece ser un error formal, pero quizás deja ver una cuestión más profunda: la desconfianza en estos sistemas.

k. ***Ausencia de valor de los programas de cumplimiento***.

Además de suprimir el Párrafo específico donde se tratan los programas de cumplimiento, la ley aprobada se aleja rotundamente del proyecto original presentado por el Ejecutivo, de las buenas prácticas promovidas por la OCDE, la UE, y las propias orientaciones y compromisos asumidos por el mismo gobierno.

En efecto, los tres gobiernos que han participado de la tramitación de esta ley han estado fuertemente comprometidos con incentivar la colaboración público-privada en materia de protección de datos, y en ese sentido, los programas de compliance son una poderosa herramienta para este propósito. Ahora bien, para que las empresas inviertan y sustenten programas potentes de cumplimiento y prevención, el Estado debe generar incentivos, y

los incentivos normativos, especialmente en materia infraccional son los más eficientes, y costo efectivo para el Estado. Existe abundante evidencia que demuestra lo anterior.

Siendo así, el proyecto propuesto por el Ejecutivo, y que fuera aprobado en general por el Senado contemplaba un incentivo para que las empresas implementaran estos programas de cumplimiento; así, aquellas empresas que contaran con estos programas y, eventualmente incurrieran en una infracción leve, grave o gravísima, se entenderá a su respecto que cuentan con una atenuante calificada, por haber cumplido fehacientemente sus deberes de dirección y supervisión para la protección de los datos personales bajo su responsabilidad o tratamiento, previa certificación de la Agencia.

No es razonable que se aplique el mismo tratamiento a una empresa que no ha hecho ningún esfuerzo de prevención, frente a otra que ha desarrollado todo un programa de prevención y cumplimiento. Sin embargo, el actual texto de la ley N°21.719, eliminó la regla que contenía esta atenuante especial.

¿Qué incentivo podrá tener hoy una empresa, una corporación, una universidad, etc., para invertir y desarrollar un plan de prevención de infracciones y cumplimiento en materia de datos personales?

1 ***Vigencia de la ley***.

El artículo primero transitorio de la ley N°21.719 establece que la nueva ley de datos personales entra en vigencia el día primero del mes vigésimo cuarto posterior a la publicación de la ley en el Diario Oficial, esto es, el **1 de diciembre de 2026.** La vacancia definida fue de dos años. El proyecto de ley aprobado por el Senado en el primer trámite constitucional estableció una vacancia de un año.

Luego de siete años y medio de tramitación, aumentar el período de vacancia de la ley resulta inexplicable.

En principio hace sentido rebajar este plazo, pero considerando el tiempo que podría durar la tramitación de este proyecto de ley, puede perder pertinencia una modificación de esta materia.

Por tanto, con base en todos los antecedentes, consideraciones y fundamentos expuestos; vengo en someter a vuestra consideración el siguiente proyecto de ley:

Proyecto de ley que modifica la ley N° 21.719, regula la protección y el tratamiento de los datos personales y crea la Agencia de protección de datos personales, adecuándola a estándares compatibles con la economía digital

Artículo único: Introdúcense las siguientes modificaciones a la ley N°21.719, regula la protección y el tratamiento de los datos personales y crea la Agencia de protección de datos personales:

1. Suprímese el artículo 1º bis.

2. Modificase el artículo 2º en el siguiente sentido:

a. Sustitúyese la letra g) por la siguiente:

> ***g) Datos personales sensibles****: tendrán esta condición aquellos datos que revelen el origen étnico o racial, las opiniones políticas, las convicciones ideológicas o filosóficas, las creencias religiosas, la afiliación sindical, los datos relativos a la salud, al perfil biológico humano, los datos biométricos, y la información relativa a la vida sexual, a la orientación sexual y a la identidad de género de una persona natural.*

b. Reemplázase la letra i) por la siguiente:

> *"**i) Fuentes de acceso público**: todas aquellas bases de datos o conjuntos de datos personales, públicos o privados, cuyo acceso o consulta puede ser efectuada en forma licita por cualquier persona, tales como el Diario Oficial, medios de comunicación o los registros públicos que disponga la ley, siempre que no existan restricciones o impedimentos legales para su acceso o utilización.*

3. Modificase en el inciso primero del artículo 4º lo siguiente: reemplázase la coma (,) luego de la palabra *"oposición"* por una letra *"y";* y elimínanse las palabras *"y bloqueo".*

4. Reemplázase el artículo 7 por el siguiente:

*"**Artículo 7º.- Derecho de supresión**. El titular de datos tiene derecho a solicitar y obtener del responsable la supresión o cancelación de los datos personales que le conciernen, en los siguientes casos:*

a) Cuando los datos no resulten necesarios en relación con los fines del tratamiento para el cual fueron recogidos.

b) Cuando el titular haya revocado su consentimiento para el tratamiento y éste no tenga otro fundamento legal.

c) Cuando los datos hayan sido obtenidos o tratados ilícitamente por el responsable.

d) Cuando se trate de datos caducos.

e) Cuando los datos deban suprimirse para el cumplimiento de una sentencia judicial o de una obligación legal, y

f) Cuando el titular haya ejercido su derecho de oposición de conformidad al artículo siguiente y no existan otro fundamento legal para su tratamiento.

No procede la supresión cuando el tratamiento sea necesario:

i. Para ejercer el derecho a las libertades de emitir opinión y de informar.

ii. Para el cumplimiento de una obligación legal o la ejecución de un contrato suscrito entre el titular y el responsable.

iii. Por razones de interés público, especialmente en el ámbito de la salud pública.

iv. Para tratamientos con fines históricos, estadísticos o científicos y para estudios o investigaciones que atiendan fines de interés público, y

v. Para la formulación, ejercicio o defensa de una reclamación administrativa o judicial.”.

5. Sustitúyese el artículo 8º por el que se pasa a indicar:

*“**Artículo 8º.- Derecho de Oposición**. El titular de datos tiene derecho a oponerse ante el responsable a que se realice un tratamiento específico o determinado de los datos personales que le conciernan, en los siguientes casos:*

a) Si el tratamiento afecta sus derechos y libertades fundamentales.

b) Si el tratamiento se realiza exclusivamente con fines de mercadotecnia o marketing directo de bienes, productos o servicios.

c) Si el tratamiento se realiza respecto de datos obtenidos de una fuente de acceso público y no exista otro fundamento legal para su tratamiento.

e) Si el tratamiento se realiza para la satisfacción de intereses legítimos del responsable o terceros, y con ello se afectan sus derechos o libertades.

No procederá la oposición al tratamiento de datos por las mismas causales señaladas en los numerales i. al iv. del artículo anterior. ”.

6. Reemplázase el artículo 8° bis por el siguiente:

*“**Artículo 8° bis. - Derecho de oposición a valoraciones personales automatizadas**. El titular de datos tiene derecho a oponerse a que el responsable adopte decisiones que le conciernan basadas únicamente en el hecho de realizarse a través de un tratamiento automatizado de sus datos personales, incluida la elaboración de perfiles.*

El titular no podrá ejercer este derecho de oposición en los siguientes casos:

a) Cuando la decisión del responsable sea necesaria para la celebración o ejecución de un contrato entre el titular y el responsable;

b) Cuando exista consentimiento previo y expreso del titular, y

c) Cuando lo disponga la ley.

En los casos de las letras a) y b) del inciso anterior, el responsable deberá adoptar las medidas necesarias para asegurar los derechos del titular de datos consagrados en esta ley, y en particular, los derechos a obtener intervención humana por parte del responsable, a expresar su punto de vista, y a solicitar la revisión de la decisión adoptada.".

7. Suprímese el artículo 8º ter.

8. Eliminase el inciso segundo del artículo 10º.

9. Modificase el artículo 13 del modo que se pasa a indicar:

   a. Agrégase una letra a) nueva del siguiente tenor:

      "a) Cuando los datos han sido recolectados de una fuente de acceso público y su tratamiento esté relacionado con los fines para los cuales fueron entregados o recogidos.".

   b. Reordénanse las letras siguientes, pasando la actual a) a ser b) y así sucesivamente.

10. Eliminase de la letra a), del inciso primero del artículo 24, el siguiente párrafo: *"Respecto de los datos que se realicen con esta finalidad, no será aplicable lo dispuesto en el artículo 25.". ''*

11. Agrégase en el inciso segundo del artículo 27, la siguiente letra i) nueva:

      "i) Cuando la transferencia se efectúe entre sociedades o entidades que pertenezcan a un mismo grupo empresarial, empresas- relacionadas o

sujetas a un mismo controlador en los términos previstos en la Ley de Mercado de Valores, siempre que todas ellas operen bajo los mismos estándares y políticas en materia de tratamiento de datos personales. El responsable que efectúe la transferencia de datos asumirá la responsabilidad por cualquier infracción a los estándares y políticas corporativas vinculantes en que incurra algunos de los miembros del grupo empresarial. El responsable sólo podrá exonerarse de esta responsabilidad cuando acredite que la infracción no fue imputable al miembro del grupo empresarial correspondiente.".

12. Modificase el artículo 35 según se pasa a indicar:

a. Reemplázanse en el inciso primero del artículo 35. las letras a), b) y c) por 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, y

c) Las infracciones gravísimas serán sancionadas con multa de 1.00J a 5.000 unidades tributarias mensuales.".

b. Sustitúyense los incisos segundo, tercero y cuarto por los siguientes:

"Conjuntamente con aplicación de la sanción pecuniaria, la Agencia señalará las medidas tendientes a subsanar la infracción que le dio origen; e infractor deberá adoptar las medidas de corrección en un plazo no mayor a sesenta días, salvo que existan motivos justificados, en caso contrario, se le impondrá una nueva multa, con un recargo del 50% respecto del monto de la mulla originalmente cursada.

Si existiera reincidencia en los términos previstos en el literal a) del inciso segundo del artículo 36, la Agencia podrá aplicar hasta el duplo de la

multa asignada originalmente a la infracción cometida.

Cuando el infractor corresponda a una empresa distinta de aquellas definidas como empresas de menor tamaño según lo dispuesto en el artículo 2° de la ley N° 20.416, y reincida en una infracción grave o gravísima, la multa podrá alcanzar al triple de la multa original asignada o hasta el monto equivalente al 2% de los ingresos anuales por ventas y servicios y otras actividades del giro de la empresa en el último año calendario, según lo determine la Agencia.".

13. Introdúcense las siguientes enmiendas al artículo 37:

a) Suprímese el numeral 8.- del inciso primero.

b) Agréganse los siguientes incisos segundo y tercero, nuevos, reordenándose los siguientes:

"La Agencia de Protección de Datos Personales deberá ponderar racionalmente cada una de las atenuantes y agravantes con el objeto de aplicar, al caso concreto, una multa proporcional a la intensidad de la afectación.

Con todo, cuando concurran las circunstancias atenuantes establecidas en los números 4) o 5) del artículo anterior, la Agencia podrá aplicar el rango inferior de la sanción definida para el tipo de infracción cometida, o su exoneración, esto último, salvo que se trate de una infracción gravísima.".

14. Agrégase al Título VII, un nuevo epígrafe, que antecede a los artículos 48 y siguientes, con la siguiente denominación:

"Párrafo Sexto
De los Modelos de Prevención de Infracciones"

15. Reemplázánce los artículos 49, 50 y 51 por los siguientes:

a. Artículo 49:

*"**Artículo 49.- Modelo de prevención de infracciones**. Los responsables de datos podrán voluntariamente adoptar un modelo de prevención de infracciones. Configuran un modelo de prevención de infracciones cualesquiera de los siguientes mecanismos o instrumentos:*

a) La designación de un encargado de prevención o delegado de protección de datos personales.

Los órganos públicos que establezcan un encargado de prevención o delegado de protección de datos personales deberán designar para ello a un funcionario de la dotación vigente del respectivo organismo.

b) La adopción de un programa de cumplimiento o de prevención de infracciones.

b. Artículo 50:

*"**Artículo 50.- Encargado de prevención o delegado de protección de datos**. El responsable de datos podrá designar un encargado de prevención o delegado de protección de datos personales*

El encargado o delegado de protección de datos deberá ser designado por la máxima autoridad directiva o administrativa del responsable de datos. Se considerará como la máxima autoridad directiva o administrativa al directorio, un socio administrador o a la máxima autoridad de la empresa o servicio, según corresponda.

El encargado o delegado de protección de datos deberá contar con autonomía respecto de la administración, en las materias relacionadas con esta ley. En las micro, pequeñas y medianas empresas, el dueño o sus máximas autoridades podrán asumir personalmente las tareas de encargado de prevención o delegado de protección de datos.

El encargado de prevención o delegado de protección de datos podrá

desempeñar otras funciones o cometidos dentro de la empresa o institución. El responsable garantizará que dichas funciones y cometidos no den lugar a conflicto de intereses.

La designación del encargado de prevención o delegado de protección de datos debe recaer en una persona que reúna los requisitos de idoneidad, capacidad y conocimientos específicos para el ejercicio de sus funciones.

Los titulares de datos podrán ponerse en contacto con el encargado de prevención o delegado de protección de datos en lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos al amparo de esta ley.

El encargado de prevención de datos estará obligado a mantener estricto secreto o confidencialidad de los datos personales que conociere en ejercicio de su cargo. Los funcionarios públicos que desempeñen estas funciones e infrinjan este deber de secreto o confidencialidad, serán sancionados de conformidad a lo que se prescribe en los artículos 246 a 247 bis del Código Penal. El responsable se hará cargo por las infracciones al deber de secreto o confidencialidad que debía cumplir su encargado de prevención o delegado de protección, sin perjuicio de las acciones de repetición que pueda ejercer contra éste.

El responsable de datos deberá disponer que el encargado o delegado cuente con los medios y facultades suficientes para el desempeño de sus funciones, otorgándole los recursos materiales necesarios para realizar adecuadamente sus labores, en consideración al tamaño y capacidad económica de la entidad.

Sin perjuicio de otras funciones que se le puedan asignar, el encargado de prevención o delegado de protección de datos tendrá las siguientes:

a) *Informar y asesorar al responsable de datos, a los terceros encargados o mandatarios y a los dependientes del responsable, respecto de las disposiciones legales y reglamentarias relativas al derecho a la*

protección de los datos personales y a la regulación de su tratamiento.

b) *Promover y participar en la política que dicte el responsable de datos respecto de la protección y el tratamiento de los datos personales.*

c) *Supervisar el cumplimiento de la presente ley y de la política que dicte el responsable, dentro del ámbito de su competencia.*

d) *Preocuparse de la capacitación y formación permanente de las personas que participan en las operaciones de tratamiento de datos.*

e) *Desarrollar un plan anual de trabajo y rendir cuenta de sus resultados.*

fi Absolver las consultas y solicitudes de los titulares de datos.

g) Cooperar y actuar como punto de contacto de la Agencia.".

c. Artículo 51:

*"**Artículo 51.- Programa de cumplimiento o de prevención de infracciones**. Los responsables de datos podrán adoptar programas de cumplimientos o de prevención de infracciones, los que deberán contener, a los menos, los siguientes elementos:*

a) Designación de un encargado de prevención o delegado de protección de datos personales.

b) Definición de medios y facultades del encargado de prevención o delegado de protección de datos.

c) Establecimiento de un programa de cumplimiento que deberá contemplar, a lo menos, lo siguiente:

i. La identificación del tipo de información que la entidad trata, el ámbito territorial en que opera, la categoría, clase o tipos de

datos o bases de datos que administra, y la caracterización de los titulares de datos.

ii. La identificación de las actividades o procesos de la entidad sean habituales o esporádicos, en cuyo contexto se genere o incremente el riesgo de comisión de las infracciones señaladas en los artículos 34 bis, 34 ter y 34 quater.

iii. El establecimiento de protocolos, reglas y procedimientos específicos que permitan a las personas que intervengan en las actividades o procesos indicados en la letra anterior, programar y ejecutar sus tareas o labores de una manera que prevenga la comisión de las referidas infracciones.

iv. Mecanismos de reporte hacia las autoridades para el caso de contravenir lo dispuesto en la presente ley.

v. La existencia de sanciones administrativas internas, así como de procedimientos de denuncia o castigo de responsabilidades de las personas que incumplan el sistema de prevención de infracciones.

d) Supervisión y certificación del programa de cumplimiento o de prevención de infracciones.

La regulación interna a que dé lugar la implementación del programa, en su caso, deberá ser incorporada expresamente como una obligación en los contratos de trabajo o de prestación de servicios de todos los trabajadores, empleados y prestadores de servicios de las entidades que actúen como responsables de datos o los terceros que efectúen el tratamiento, incluidos los máximos ejecutivos de la misma, o bien, como una obligación del reglamento interno del que tratan los artículos 153 y siguientes del Código del Trabajo. En este último caso, se deben realizar las medidas de publicidad establecidas en el artículo 156 del mismo Código.

Las sociedades o entidades que pertenezcan a un mismo grupo empresarial, empresas relacionadas o sujetas a un mismo controlador en los términos previstos en la Ley de Mercado de Valores, podrán contar con un mismo modelo de un cumplimiento y designar un único encargado de prevención o delegado de protección de datos, siempre que todas ellas operen bajo los mismos estándares y políticas en materia de tratamiento de datos personales, y el encargado o delegado sea accesible para todas las entidades y establecimientos del grupo empresarial. ”.