Mayo 4, 2022

HONORABLES DIPUTADAS Y DIPUTADOS
COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO
CÁMARA DE DIPUTADAS Y DIPUTADOS DE CHILE

Asunto: Comentarios de ALAI al Proyecto de Ley que *Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales,* boletines refundidos N°s 11.144-7 (S) y 11.092-07(S).

Por medio de la presente, les hacemos extensivo un cordial saludo en nombre de la Asociación Latinoamericana de Internet (ALAI), organización regional sin fines de lucro que trabaja por el desarrollo digital de Latinoamérica desde la perspectiva de la industria de Internet. ALAI respalda políticas que favorezcan el respeto y ejercicio de los derechos humanos, el emprendimiento y la innovación.

Los miembros asociados de ALAI son empresas regionales latinoamericanas o empresas globales con fuerte presencia en Latinoamérica, que son nacidas de Internet o han evolucionado sus modelos de negocio a modelos basados en el funcionamiento de Internet. Las empresas miembro de ALAI trabajan permanentemente para mantener la confianza de sus clientes, quienes confían su información, incluidos sus datos personales, a nuestros miembros asociados. Como resultado, la protección de los datos, la privacidad y la seguridad de los usuarios son pilares fundamentales de las operaciones de nuestra asociación.

Celebramos los esfuerzos de esta Comisión por avanzar en una nueva reglamentación de protección y tratamiento de datos que se ajuste a los desafíos actuales y futuros. No obstante, estimamos que es importante realizar los ajustes sugeridos en este documento, detallados a continuación, con el fin de que el Proyecto de Ley cumpla el objetivo de robustecer y modernizar la protección de datos personales en Chile, sin imponer cargas desproporcionadas a los responsables y/o encargados del tratamiento de datos que impacten negativamente el desarrollo digital chileno. Esperamos que estas observaciones contribuyan al desarrollo del texto normativo y ofrecemos nuestra colaboración para seguir avanzando en este proceso.

En nombre de ALAI, agradecemos la oportunidad de proporcionar nuestros comentarios. De antemano, muchas gracias por su atención.

Saludos cordiales,

Raúl Echeberría
Director Ejecutivo
Asociación Latinoamericana de Internet - ALAI

COMENTARIOS A PROYECTO DE LEY DE PROTECCIÓN DE DATOS PERSONALES TEXTO APROBADO POR EL SENADO EN 1ER TRÁMITE CONSTITUCIONAL

COMENTARIO GENERAL:

Sacar adelante una ley de protección de datos personales acorde a desafíos actuales y futuros es favorable para el desarrollo digital, económico y social chileno. Por un lado, es fundamental proveer una base sólida de protección a la privacidad de los usuarios, quienes cada vez más exigen mayores garantías. Por otro lado, una ley de protección de datos adecuada puede ofrecer mayor certeza jurídica, claridad y previsibilidad a empresas de todo tipo, especialmente aquellas que utilizan el tratamiento de datos para el desarrollo de soluciones innovadoras.

Así, entendemos que es positiva y necesaria la creación de una agencia de protección de datos en Chile. No obstante, para que esta funcione correctamente, no solo se debe garantizar su independencia, sino también su competencia exclusiva y excluyente sobre la interpretación de la Ley.

Uno de los desafíos ocasionados por la ausencia de una autoridad de protección de datos a la fecha es que otros organismos de control, motivados por buenas intenciones de velar por la protección de los usuarios, han intentado cubrir algunos espacios que hasta hoy son desatendidos por la misma ausencia de una agencia de protección de datos. La propuesta de creación de una agencia de protección de datos, entonces, no solo debe buscar cubrir espacios desatendidos, sino que debe evitar traslapes entre las facultades de los actuales organismos de control y la futura agencia de protección de datos, garantizando una gobernanza de la protección de datos personales clara, con facultades debidamente delimitadas y evitando el riesgo de sobrerregulaciones.

En consecuencia, estimamos que resulta fundamental que el Proyecto de Ley sea explícito en señalar claramente la competencia exclusiva y excluyente de la nueva agencia de protección de datos personales sobre la interpretación de la Ley .

COMENTARIOS ESPECÍFICOS:

1. **ARTÍCULO 1°: N° 4:** modificaciones al Art. 2° de la Ley N° 19.628.

a) Se incluye la **letra f)**, que contiene la definición de "*dato personal*" y por separado, el artículo 16 sexies introduce los datos de geolocalización (el cual podrá ser realizado bajo las fuentes de licitud establecidas en la ley). Sugerimos incluir dentro de la definición de "*datos personales*" a los "*datos de geolocalización*" y eliminar el artículo 16 sexies, en tanto es innecesario que cuenten con un artículo diferenciado cuando aplican las mismas bases legales para su tratamiento.

b) Sugerimos modificar la nueva **letra g)**, "*datos personales sensibles*" y eliminar el concepto de "*hábitos personales*". La definición resulta demasiado amplia, teniendo en cuenta que podría incluir cualquier comportamiento de una persona, e incluir a cualquier tipo de dato dentro de la categoría de datos sensibles. Además, dentro de la definición de datos sensibles se incluyen los datos biométricos. Sin embargo,

no todo dato biométrico es necesariamente un dato sensible. Creemos conveniente limitar la inclusión de dato biométrico como dato sensible de la misma forma que lo hace el Reglamento General de Protección de Datos europeo (RGPD), es decir, cuando se sometan a un tratamiento técnico específico dirigido a identificar de manera unívoca a una persona física.

c) Se propone una nueva **letra k)**, que sustituye a la actual letra l), reemplazando en consecuencia la definición de anonimización o disociación, señalando que es un "*procedimiento irreversible en virtud del cual un dato personal no puede vincularse o asociarse a una persona determinada, ni permitir su identificación, por haberse destruido o eliminado el nexo con la información que vincula, asocia o identifica a esa persona. Un dato anonimizado deja de ser un dato personal*".

   Esta definición necesita ser revisada: la información "*disociada*" por definición puede ser reversada con datos adicionales y medidas técnicas, pero se puede hacer en base al propio texto de la ley. Por lo mismo, se sugiere eliminar el concepto de disociación y que la definición corresponda al concepto de anonimización.

d) Las modificaciones también contemplan un nuevo **literal x)** que agrega una definición de motor de búsqueda. Esta es una definición que aparece como innecesaria y que debería eliminarse debido a que no se utiliza el término definido en el articulado del proyecto. Por lo demás, todos los actores que se encuentran en una misma situación deberían estar sujetos a una misma regulación, evitando así un trato discriminatorio que pueda tener efectos anticompetitivos.

   La jurisprudencia ha resuelto que los motores de búsqueda no son responsables por la verificación del contenido creado y publicado por terceros, ya que los motores de búsqueda solo permiten encontrar dicho contenido. Por ejemplo, la Corte Suprema ha resuelto que los buscadores no reúnen las condiciones para ser considerados responsables del tratamiento de datos personales.[1] En este sentido, los motores de búsqueda se encuentran en una situación análoga a los proveedores de acceso a Internet, que cuentan actualmente con una normativa en vigor que limita su responsabilidad en casos de eventuales infracciones al derecho de autor cometidas por sus suscriptores (Artículos 85L a 85U de la Ley N° 17.336).

   En esta línea, la indicación 132 (Ejecutivo) presentada durante la discusión legislativa del Proyecto en el Senado, hace un distinción que es correcta, al separar los roles de intermediarios y de responsables, ya que tienen naturaleza diferente.[2] Se sugiere que la norma deje establecido claramente que se trata de personas que

[1] Un motor de búsqueda no es "*el creador de los contenidos publicitados en internet (…). En efecto, (…) un motor de búsqueda (…) no le corresponde (…) verificar la verdad de la información que se transmite, no dispone almacenarla o publicarla, ni tampoco tiene autoridad para hacerla excluir (…)" (*Página N°6 y siguientes, Excelentísima Corte Suprema, Rol: 22.243-2015.)

[2] "Artículo …- Prestación de servicios para el tratamiento de datos. Las personas naturales o jurídicas que presten servicios de infraestructura, plataforma, software u otros servicios para el almacenamiento o procesamiento de los datos, o para facilitar enlaces o instrumentos de búsqueda, no tendrán la calidad de responsables de datos para los efectos de esta ley, salvo que tomen decisiones acerca de los medios y fines del tratamiento de datos, en cuyo caso responderán por el tratamiento que hayan realizado de acuerdo a las normas previstas en esta ley para los responsables de datos, sin perjuicio de las demás responsabilidades y sanciones que les puedan caber por incumplimiento de contratos o infracciones legales."

no tienen el control de los datos respecto de los cuales se utilizan sus servicios y en consideración a lo mismo responden únicamente de aquellos tratamientos específicos respecto de los cuales sí tomaron decisiones respecto de medios o finalidad.

2. **ARTÍCULO 1° N° 4:** modificaciones al Título I, se propone un nuevo **artículo 4** sobre los derechos del titular de datos, por medio del cual faculta a los herederos a ejercer los derechos del titular del dato fallecido. Sin embargo, no queda claro en qué situaciones los herederos pueden ejercer los derechos en nombre de la persona fallecida (si pueden hacerlo sin que sea necesaria una justificación o si pueden hacerlo únicamente cuando exista el interés legítimo del representante o de la persona fallecida para ejercer este derecho). Teniendo en cuenta la amplitud de las situaciones en las que los herederos podrán ejercer estos derechos, sugerimos modificar el texto de la siguiente manera: "*En caso de fallecimiento del titular de datos, los derechos que reconoce esta ley pueden ser ejercidos por sus herederos, siempre que exista un interés legítimo por parte de este, y de acuerdo con la ley aplicable*".

3. **ARTÍCULO 1° N° 6:** modificaciones al Título I, se propone sustituir el **artículo 5°** de la Ley N° 19.628 por un nuevo artículo 5° que regula el derecho de acceso. En su inciso primero se detalla la información que tendrá que entregar el responsable al titular de los datos que ejerza su derecho de acceso, indicando en la letra a) los datos tratados y su origen.

   Se propone eliminar de dicha letra a) el origen de los datos tratados, o al menos precisar esta obligación siguiendo la regulación del RGPD, que establece respecto del derecho de acceso que la información disponible sobre el origen de los datos recolectados solo se debe informar cuando no se hayan obtenido del titular (art. 15). Además, sugerimos que se defina lo que se entiende por "*esfuerzo desproporcionado*".

4. **ARTÍCULO 1° N° 6:** modificaciones al Título I, se propone un nuevo **artículo 6°**, que consagra el derecho de rectificación y la obligaciones de los responsables de comunicar dichos cambios o rectificaciones a las personas o entidades a las cuales se les hayan comunicado o cedido los datos personales. Teniendo en cuenta que pueden existir situaciones en donde resulte imposible informar cada rectificación por parte de los usuarios, es necesario que existan excepciones. En este sentido, se sugiere incluir en el requisito que dicha comunicación tendrá lugar siempre que sea posible o no requieran un esfuerzo desproporcionado.

5. **ARTÍCULO 1° N° 6:** modificaciones al Título I, propone establecer una norma que contempla el derecho de cancelación en los siguientes términos: "***Artículo 7°***.- *Derecho de cancelación. El titular de datos tiene derecho a solicitar y obtener del responsable la cancelación o supresión de los datos personales que le conciernen, especialmente en los siguientes casos*, […]"

   Recomendamos modificar esta disposición, determinando las causales concretas por las que procederá solicitar la cancelación. Es preferible una enumeración taxativa, ya que proporciona seguridad y previsibilidad. En ese sentido, sugerimos

considerar que el artículo 17 del RGPD señala un listado cerrado de causales legales, limitando el ejercicio de este derecho a los casos definidos en la norma.

Adicionalmente, recomendamos incorporar en las limitaciones al ejercicio del derecho de cancelación en Chile las siguientes: (i) que sea precedido de una sentencia judicial; (ii) que sea aplicado a la fuente que genera la información; (iii) que queden excluidas del ámbito de aplicación del derecho al olvido las personas del ámbito público; y (iv) que quede excluido del ámbito de aplicación del derecho al olvido los delitos de alta connotación pública.

Por último, observamos que la actual redacción podría interpretarse como contraria al Artículo 13.3 de la Convención Americana sobre Derechos Humanos, ya que podría entenderse como una forma de censura indirecta.

6. **ARTÍCULO 1° N° 6:** modificaciones al Título I, contempla, en su **artículo 8°**, un derecho de oposición. Sobre este punto, observamos que el procedimiento prescrito incluye la posibilidad de establecer un bloqueo temporal que se asemeja a una medida cautelar que, por su naturaleza gravosa, en nuestro sistema requiere de la intervención de un juez, pero que en este caso es dejada al arbitrio entre particulares. Idealmente, con el objetivo de que sea un procedimiento eficaz, la ley debería limitarse a ordenar el establecimiento de un procedimiento para obtener el objetivo deseado, no a establecer el procedimiento en sí.

   Asimismo, el derecho de oposición, tal como está escrito, incluye un derecho amplio para que las personas rechacen el procesamiento de datos personales de "*fuentes disponibles públicamente*" (literal c del Artículo 8°), lo que tendría amplias implicaciones tanto en la industria tecnológica como en muchos otros campos. Por ejemplo, es posible que los investigadores, periodistas y los formuladores de políticas públicas ya no puedan usar los datos de censos para una amplia gama de aplicaciones.

7. **ARTÍCULO 1° N° 6:** modificaciones al Título I, se propone un nuevo **artículo 8° bis,** que consagra el derecho de oposición a valoraciones personales automatizadas.

   La disposición debería hacer referencia a efectos o consecuencias derivadas del procesamiento que se avenga a un determinado umbral de gravedad. Una alternativa para lograr dicho objetivo es la introducción de un lenguaje similar al utilizado en el Art. 22 del RGPD: "*…que produzca efectos jurídicos en él o le afecte significativamente de modo similar*" al final de la primera frase. Esto distinguiría el uso de procesos automatizados rutinarios con efectos insustanciales de otros efectos sustantivos y gravosos.

   De igual modo, consideramos que la disposición debe ser aplicable sólo en el caso de procesamiento totalmente automatizado. Si es posible algún tipo de intervención humana, no debería haber necesidad de someter este tipo de toma de decisiones a un estándar diferente. Por lo tanto, incluir "*totalmente*" en el primer párrafo antes de "*automatizado*" y después de "*a través de*", podría ser una forma

efectiva de abordar esta inconsistencia.

8. **ARTÍCULO 1° N° 7:** modificaciones al Título II, se propone un nuevo **artículo 12**, en donde se establece el consentimiento de manera separada a otras bases legales para el tratamiento de datos personales. Esto resulta inadecuado ya que todas las bases legales para el tratamiento gozan del mismo nivel de relevancia y, por ende, deberían ser enunciadas en un mismo artículo. Es importante señalar que en otras legislaciones de protección de datos personales, como el RGPD o la Ley General de Protección de Datos brasileña (LGPD), ya no se establecen excepciones al consentimiento, sino otras bases legales las cuales se equiparan al consentimiento. En ese sentido, sugerimos unificar los artículos 12 y 13, de modo que todas las fuentes tengan el mismo grado de validez, y que el responsable del tratamiento pueda decidir qué base legal utilizar para el tratamiento específico. Respetuosamente, sugerimos el siguiente texto para unificar los artículos 12 y 13:

   "*"Artículo 12 - Fuentes de licitud del tratamiento de datos". El tratamiento sólo será lícito cuando:*

   - *El titular del dato dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;*
   - *Los datos han sido recolectados de una fuente de acceso público;*
   - *El tratamiento esté referido a datos relativos a obligaciones de carácter económico, financiero, bancario o comercial y se realice de conformidad con las normas del Título III de esta ley;*
   - *El tratamiento sea necesario para la ejecución o el cumplimiento de una obligación legal o lo disponga la ley;*
   - *El tratamiento de datos sea necesario para la celebración o ejecución de un contrato entre el titular y el responsable, o para la ejecución de medidas precontractuales adoptadas a solicitud del titular;*
   - *El tratamiento sea necesario para la satisfacción de intereses legítimos del responsable o de un tercero, siempre que con ello no se afecten los derechos y libertades del titular. En todo caso, el titular podrá exigir siempre ser informado sobre el tratamiento que lo afecta y cuál es el interés legítimo en base al cual se efectúa dicho tratamiento;*
   - *El tratamiento de datos sea necesario para la formulación, ejercicio o defensa de un derecho ante los tribunales de justicia. El responsable deberá acreditar la licitud del tratamiento de datos;*
   - *El tratamiento sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;*
   - *El tratamiento sea necesario para proteger intereses vitales del interesado o de otra persona física.*"

9. **ARTÍCULO 1° N° 7:** modificaciones al Título II, se propone un nuevo **artículo 13**, que establece otras fuentes de licitud de tratamiento de datos. Acá se incluye en la letra e) el interés legítimo del responsable o de un tercero para justificar la necesidad del tratamiento, señalando que aplica siempre que con ello no se afecten los "*derechos y libertades del titular*".

Esta referencia debería ser más precisa. Se sugiere guiarse por el texto del considerando 47 del RGPD, que establece la misma regla pero modera la referencia a los "*intereses o derechos y libertades del interesado (titular)*" señalando que debe tenerse en cuenta las "*expectativas razonables de los interesados basadas en su relación con el responsable (del tratamiento)*".

10. **ARTÍCULO 1° N° 7:** modificaciones al Título II, se propone el **artículo 14**, sobre las obligaciones del responsable de datos. Sugerimos simplificar la redacción del inciso a), reemplazandola por la siguiente: "*Poner a disposición del titular los antecedentes que acrediten la licitud del tratamiento de datos que realiza, cuando sea requerido*".

11. **ARTÍCULO 1° N° 7:** modificaciones al Título II, se propone un nuevo **artículo 14 ter**, el cual establece que el responsable del tratamiento debe mantener permanentemente a disposición del público, en su sitio web o en cualquier otro medio de información, la individualización del responsable de datos y su representante legal y la identificación del encargado de prevención, si existiere. La obligación de incluir el nombre específico del representante legal o encargado de prevención puede vulnerar la privacidad y seguridad del individuo, de modo que el carácter público de dicha información en un sitio concurrido puede generarle daños o perjuicios. Con el fin de proporcionar un contacto a los individuos, es recomendable que se publique el nombre o contacto del área encargada de atender cuestiones relacionadas a la privacidad. En este sentido, se sugiere sustituir el inciso b) por el siguiente texto: "*La individualización del responsable de datos y la información de contacto del área encargada de cuestiones de privacidad.*"

12. **ARTÍCULO 1° N° 7:** modificaciones al Título II, se propone un nuevo **artículo 14 quinquies**, que consagra un deber del responsable de los datos de adoptar medidas de seguridad. En el inciso segundo se propone que si las bases de datos que opera el responsable tienen distintos niveles de riesgo, el responsable deberá adoptar las medidas de seguridad que correspondan al nivel más alto.

    Se sugiere que este inciso segundo sea eliminado. El mantenerlo forzaría a todas las bases de datos a tener el mismo nivel de protección, incluso cuando existan distintos tipos de datos y de riesgos involucrados. Si el responsable queda obligado a establecer las medidas más estrictas de seguridad sin considerar los niveles de riesgo asociados, en la práctica se está obligando a todos los responsables a tener un solo nivel de seguridad, lo que podría resultar precisamente en menores niveles de protección. Esto, ya que para poder cumplir con el requisito, el responsable podría resultar igualando los niveles de protección de las bases de datos a niveles más bajos. Así, se debe tener en consideración que niveles distintos de protección normalmente implican diferencias sustanciales en los costos, recursos y capacidades en la operación de los responsables. Además, la redacción actual de este artículo es contradictoria respecto del artículo 14 quáter, puesto que el mencionado deber de protección desde el diseño y por defecto implica un análisis de distintos niveles de riesgo y la aplicación de medidas atenuantes de acuerdo a esos niveles de riesgo.

13. **ARTÍCULO 1° N° 7:** modificaciones al Título II, se propone un nuevo **artículo 14 sexies**, que consagra el deber de reportar las vulneraciones a las medidas de seguridad. En su inciso tercero se regula la comunicación y notificación que debe efectuar el responsable en relación con datos personales sensibles, de menores de 14 años o datos relativos a obligaciones de carácter económico, financiero, bancario o comercial.

    Al respecto, debe tenerse presente que la obligación de notificación al titular de los datos en caso de vulneraciones a las medidas de seguridad no debería estar basada en el tipo de datos (en este caso, datos sensibles, de menores de 14 años y relativos a obligaciones económicas, financieras, bancarias o comerciales) sino en el riesgo efectivo de vulneración. Si se vulnera una base de datos que solo contiene datos pseudonimizados, el riesgo es muy bajo. Acá nuevamente se sugiere seguir el enfoque del RGPD y proponer que la notificación a los titulares se haga solo cuando existe un riesgo alto para los titulares (art. 34 N° 1 RGPD). Por este motivo, sugerimos eliminar el tercer párrafo o modificarlo para que se base en el riesgo efectivo de vulneración y no en el tipo de datos. Además, es recomendable que se ofrezca más información sobre lo que corresponde a "*un riesgo razonable para los derechos y libertades de los titulares*", para que se tenga más seguridad jurídica sobre cuando es necesario reportar a la Agencia.

14. **ARTÍCULO 1° N° 7:** modificaciones al Título II, se propone un nuevo **artículo 15** que regula la cesión de datos personales. En su inciso primero, se reconocen fuentes legales específicas para la cesión por las cuales no es necesario obtener el consentimiento del titular (cuando la cesión es necesaria para el cumplimiento y ejecución de un contrato en que es parte el titular, cuando exista un interés legítimo del cedente o del cesionario, y cuando lo disponga la ley). No es conveniente hacer mención a una fuente de licitud específica para la cesión ya que esto podría conducir a incertidumbres innecesarias. La fuente legal debería ser la misma que la reconocida para cualquier tratamiento de datos (art. 13 del Proyecto) y la única limitación debería ser la exigencia de mecanismos de seguridad para evitar la vulneración de los datos cedidos.

15. **ARTÍCULO 1° N° 7:** modificaciones al Título II, se propone un nuevo **artículo 15 bis** que regula el tratamiento de datos a través de un tercero mandatario o encargado.

    El inciso cuarto dispone que en caso de una vulneración a las medidas de seguridad, el encargado deberá reportar este hecho a la Agencia y al responsable. En cuanto a esta obligación, cabe señalar que esto puede dar lugar a conflictos entre responsables y encargados, ya que la evaluación de si existe o no una vulneración a las medidas de seguridad puede ser llevada a cabo de forma diferente por el encargado que por el responsable. Se recomienda adoptar el enfoque del RGPD, según el cual los encargados tienen la obligación exclusiva de informar de tales vulneraciones al responsable (artículo 33.2 RGPD).

    El inciso final propuesto dispone que cumplida la prestación del servicio de tratamiento por parte del tercero mandatario o encargado, los datos que obran en su poder deberán ser cancelados o devueltos al responsable de datos, según corresponda. Se propone incorporar una modificación a esta norma que le permite

a los terceros mandatarios o encargados retener los datos que deben ser cancelados o devueltos al responsable cuando así la ley lo exija, cuando la relación con el responsable haya cesado. Por ejemplo, el art. 28 letra g) del RGPD dispone que el encargado del tratamiento debe suprimir o devolver los datos personales, a elección del responsable, cuando finalice la prestación de los servicios de tratamiento, "*a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros*."

16. **ARTÍCULO 1° N° 7:** modificaciones al Título II, se propone un nuevo **artículo 15 ter** que regula el tratamiento automatizado de "*grandes volúmenes de datos*", autorizándolo siempre que los procedimientos automatizados cautelen los derechos del titular y el tratamiento guarde relación con las finalidades autorizadas por los titulares. El Proyecto ya contempla otra norma propuesta referida a decisiones automatizadas (art. 8° bis, hay referencia en el inciso 2°), por lo que no es necesaria la creación de una regla especial para "*grandes volúmenes de datos*". Además, al referirse al artículo 12 como base de licitud para este tipo de tratamiento, se exige la obtención de consentimiento del titular, pero se permite también el tratamiento en base a las fuentes de licitud del art. 13, lo que crea confusión al no ser la única fuente lícita.

17. **ARTÍCULO 1° N° 7:** modificaciones al Título II, se propone el **artículo 16 bis** acerca de datos personales relativos a la salud y al perfil biológico humano. Este artículo incorpora restricciones a las finalidades para las cuales pueden procesarse datos de salud o datos del perfil biológico, lo cual podría representar un innecesario y arbitrario impedimento al desarrollo científico y tecnológico. Teniendo en cuenta que la ley debería representar una protección integral suficiente, cualquiera sea la finalidad, no hay necesidad de restringir las finalidades de tratamiento del perfil biológico si el tratamiento de estos datos se lleva a cabo con el cumplimiento de las bases legales establecidas en la normativa. En consecuencia, se sugiere eliminar este artículo.

18. **ARTÍCULO 1° N° 7:** modificaciones al Título II, se incluye el **artículo 16 quáter** referente a los datos personales relativos a los niños, niñas y adolescentes. Teniendo en cuenta la autonomía progresiva prevista en el artículo, se sugiere eliminar la necesidad de obtener el consentimiento de los padres o representantes legales para el tratamiento de datos sensibles de adolescentes (mayores de catorce años). Siguiendo con la línea de la autonomía progresiva, los adolescentes poseen cierto grado de madurez suficiente (lo que incluye la capacidad de prestar su consentimiento previo, expreso e informado), de manera que las normas de autorización previstas para los adultos también pueden utilizarse en este caso.

    También se sugieren como excepción al consentimiento parental (i) los casos en que el tratamiento de los datos de los niños y niñas sea necesario para contactar a los padres o representantes legales, o para su propia protección; y (ii) en el contexto de los servicios preventivos o de asesoramiento ofrecidos directamente a la niñez.

19. **ARTÍCULO 1° N° 7:** modificaciones al Título II, se propone el **artículo 16 sexies** sobre los datos de geolocalización. Tal como mencionamos en nuestro comentario

relativo al artículo de definiciones, no es necesario que los datos de geolocalización cuenten con un artículo diferenciado cuando aplican las mismas bases legales para su tratamiento, de modo que se sugiere eliminar el presente artículo e incluir el concepto de datos de geolocalización en la definición de dato personal establecida en el artículo 2.

20. **ARTÍCULO 1° N° 12:** se crean los nuevos Títulos VI, VII y VIII. En el nuevo **Título VII**, que regula las infracciones y sus sanciones, los procedimientos y las responsabilidades:

a) Sugerimos que el **artículo 30**, que dictamina la creación de la Agencia de Protección de Datos Personales, aclare de manera específica que la Agencia será la autoridad exclusiva y excluyente de interpretación de esta ley. Esto, con el fin de proveer certeza jurídica y de garantizar la autonomía e independencia de la Agencia.

b) El Párrafo 1 del Título VII incluye el **artículo 35** que establece el régimen de sanciones, en base a si la infracción es leve, grave o gravísima, y todas ellas quedan sujetas a una multa de entre 1 a 10.000 UTM, dependiendo del tipo de infracción. Solo en el caso de las infracciones leves se permite reemplazar la multa por una amonestación escrita. Al respecto, se propone introducir lenguaje que disponga que las sanciones pecuniarias solo se impondrán cuando la infracción se cometió de forma dolosa o negligente. Alternativamente, se propone incluir el dolo dentro de los criterios de determinación del monto de la multa, en su numeral 2, junto con la falta de negligencia.

c) El Párrafo 5 del Título VII se refiere a la responsabilidad civil, estableciendo en el **artículo 47** la regla general de que el responsable de los datos deberá indemnizar el daño patrimonial y extrapatrimonial que cause a los titulares, cuando en sus operaciones de tratamiento infrinja los principios, derechos y obligaciones de la ley y les cause perjuicio. Al respecto, las sanciones civiles deben ser proporcionales al daño causado a los titulares de los datos y deben considerar circunstancias atenuantes y agravantes. Además, debería establecerse una causal expresa de exención de responsabilidad, para cuando el responsable del tratamiento pueda probar que no es responsable del hecho que haya causado los daños, siguiendo lo establecido en el artículo 82.3 del RGPD.

***