BARROS SILVA VARELA & VIGIL

MINUTA

Protección de Datos Personales

&

Protección de Datos Personales

El lunes 26 de agosto el Congreso aprobó el Boletín N°1114-07, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales (“Nueva Ley de Datos Personales” o “Proyecto”). El 3 de septiembre fue remitido por el Congreso Nacional al Tribunal Constitucional para su control preventivo obligatorio. Tras esto, sería promulgado por el Presidente de la República.

La Nueva Ley de Datos Personales reforma la Ley N°19.628, sobre la Protección de la Vida Privada (“Ley N°19.628”), representa un avance significativo para la protección de la privacidad y los derechos de las personas en el manejo de sus datos personales, promoviendo una mayor transparencia y responsabilidad en el tratamiento de la información por parte de las entidades.

I. Cambios respecto a la actual regulación

La nueva ley reforma la Ley N°19.628[1] en los siguientes aspectos principales:

1. Se crea la Agencia Nacional de Protección de Datos ("Agencia"), encargada de fiscalizar el cumplimiento de la ley.

2. Se consagran nuevos derechos para el titular de datos personales, tales como el derecho a la portabilidad y oposición a decisiones automatizadas.

3. Se incluyen nuevas bases legales para el tratamiento de datos personales, como interés legítimo del responsable de datos y contratos que hayan sido ejecutados con el titular.

4. Se regula la transferencia transfronteriza de los datos personales.

5. Se establece un catálogo de infracciones gravísimas con sanciones hasta 20.000 UTM y normas especiales para la reincidencia de grandes empresas.

II. Ámbito de aplicación

Este nuevo marco normativo regula la forma y condiciones en que se efectúa el tratamiento y protección de los datos personales, se aplicará tanto a entes privados como a organismos públicos.

Asimismo, siguiendo el modelo europeo sobre la materia, se consagra un ámbito de aplicación territorial de la ley, en particular, cuando el responsable o mandatario esté establecido o constituido en el territorio nacional; cuando se haga a nombre de un tercero establecido o constituido en Chile; y cuando las operaciones de tratamiento de datos personales esté destinado a ofrecer bienes y servicios a personas en Chile[2] .

1. Del mismo modo, se introducen cambios a la Ley N°20.285, sobre acceso a la información pública (artículo segundo) y al Decreto con Fuerza de Ley N°3, de 2021, que fija texto refundido, coordinado y sistematizado de la ley N° 19.496, que establece normas sobre protección de los derechos de los consumidores (artículo tercero).

2 Asimismo, se prevé el supuesto de que se aplique la ley al responsable que trate datos personales y que, sin estar en el territorio chileno, le resulte aplicable la ley nacional por un contrato o el derecho internacional.

Asimismo, la ley consagra una serie de derechos para los titulares de datos personales, y como contrapartida, obligaciones y deberes para los responsables del tratamiento de dichos datos.

La ley distingue dos tipos de datos personales ("Datos Personales"):

(i) Datos Personales

Los datos personales son aquellos que permiten identificar o hacer identificable a una persona natural. El Proyecto consagra que se considerará "identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante uno o más identificadores". Algunos ejemplos de identificadores son:

- Nombre.
- Dirección.
- Número de identificación (como el RUT).
- Datos de localización (dirección IP, coordenadas GPS).
- Identificadores en línea (nombres de usuario, correos electrónicos).

(ii) Datos Personales Sensibles

Son una categoría especial que se refiere a características físicas, morales o a hechos y circunstancias de la vida privada de las personas. Estos datos requieren una mayor protección debido a su naturaleza, ya que se estima que una vulneración a éstos afecta la dignidad humana. Algunos ejemplos de estos son:

- Origen racial o étnico.
- Afiliación política, sindical o gremial.
- Situación socioeconómica.
- Convicciones ideológicas o filosóficas.
- Creencias religiosas.
- Datos relativos a la salud (historial médico, diagnósticos, tratamientos).
- Perfil biológico humano y datos biométricos (huellas dactilares, reconocimiento facial, ADN).
- Información sobre la vida sexual, orientación sexual e identidad de género de una persona natural.
- Situación socioeconómica[3].

III. Derechos de los titulares de datos personales

La ley busca que estos derechos puedan ser ejercidos de una manera sencilla y sin costos.

(i) Derechos establecidos en el Proyecto

(a) Derecho de acceso: permite al titular conocer quién tiene sus datos y para qué los están utilizando. El titular de los datos tiene el derecho de obtener del responsable la confirmación de si sus datos personales están siendo tratados y, en tal caso, acceder a esos datos y obtener información detallada sobre el tratamiento. Esta información incluye la fuente de los datos, la fina-

3 Cabe señalar que este dato personal sensible fue objeto de una de las 22 materias que se sometieron a Comisión Mixta en la tramitación de este Proyecto.

lidad del tratamiento, las categorías de destinatarios, el periodo de conservación y cualquier lógica aplicada en tratamientos automatizados. Este derecho garantiza la transparencia y

(b) Derecho de rectificación: esencial para mantener la precisión y actualidad de los datos personales. Este derecho permite al titular solicitar la corrección de sus datos personales cuando sean inexactos, desactualizados o incompletos. El responsable está obligado a realizar las modificaciones necesarias para asegurar que los datos sean correctos.

(c) Derecho de cancelación: También conocido como el "derecho al olvido", permite al titular solicitar la eliminación de sus datos personales en ciertos casos, como cuando los datos ya no sean necesarios para los fines para los que fueron recogidos, cuando se retire el consentimiento o cuando los datos se hayan tratado de forma ilícita.

(d) Derecho a la oposición: Permite a los individuos oponerse al tratamiento de sus datos personales cuando consideren que este afecta sus derechos o intereses. Este derecho es particularmente relevante en casos donde el tratamiento de los datos puede generar un impacto negativo en la persona, como en la elaboración de perfiles para marketing directo o en decisiones que afecten significativamente a una persona.

(e) Derecho de oposición a decisiones automatizadas: El derecho a la oposición a decisiones automatizadas permite a los individuos cuestionar y resistirse a decisiones que se han tomado exclusivamente a través de medios automatizados, sin intervención humana significativa, especialmente si estas decisiones les afectan de manera significativa. Un ejemplo de decisión automatizada son las multas por infracción a la Ley de Tránsito impuestas por una cámara.

(f) Derecho al bloqueo de los datos: El titular puede solicitar la suspensión temporal de sus datos personales en determinadas situaciones, mediante la solicitud de rectificación, supresión u oposición.

(g) Derecho a la portabilidad de los datos: Este derecho permite al titular recibir sus datos personales en un formato estructurado, de uso común y lectura mecánica, y transmitirlos a otro responsable del tratamiento sin impedimentos. Esto facilita la transferencia de datos entre diferentes servicios y proveedores.

(ii) ¿De qué forma las personas podrán ejercer estos derechos ante quienes tratan Datos Personales?

Los titulares deberán dirigirse al responsable del tratamiento de los datos personales de la respectiva entidad. Ellos estarán obligados a implementar mecanismos y herramientas tecnológicas que faciliten el ejercicio de estos derechos de forma expedita, ágil y eficaz, debiendo el responsable pronunciarse a más tardar dentro de los 30 días corridos siguientes a la fecha de su ingreso. En caso de no pronunciarse, los titulares podrán reclamar directamente ante la Agencia.

IV. Tratamiento de los Datos Personales y categorías especiales de datos

El Título II de la ley detalla las condiciones bajo las cuales las entidades pueden tratar Datos Personales de manera lícita, así como las obligaciones y deberes que deben cumplir los responsables de datos personales. Este título también clasifica los diferentes tipos de Datos Personales y establece reglas específicas para su tratamiento.

(i) Consentimiento

Como regla general, siempre se requiere el consentimiento del Titular de Datos Personales. Este consentimiento debe ser:

a) Libre.
b) Inequívoco.
c) Informado.
d) Específico.
e) De forma previa.
f) Mediante una declaración verbal o escrita.

Tratamiento. El tratamiento de datos personales es lícito en los siguientes casos:

(a) Regla general: con el consentimiento libre, informado, específico, previo y explícito. Puede ser revocado en cualquier momento, sin efectos retroactivos.

(b) Excepciones

- Sea necesario para la ejecución de un contrato en el que el titular es parte.
- Se realice en cumplimiento de una obligación legal.
- Se protejan intereses vitales del titular o de otra persona.
- Se lleve a cabo en el ejercicio de funciones públicas.
- Exista un interés legítimo del responsable, siempre que no prevalezcan los derechos del titular.

(ii) Obligaciones y Deberes de las entidades responsables del tratamiento de Datos

(a) Deber de Confidencialidad: Esto incluye proteger la información incluso después de haber terminado la relación con el titular de los datos.

(b) Deber de Transparencia: proporcionar información clara y accesible sobre la política de tratamiento de datos, incluyendo detalles como los tipos de datos que se manejan, los propósitos para los cuales se utilizan, y los derechos que tienen los titulares sobre sus datos.

(c) Deber de Seguridad: Los responsables de datos deben implementar medidas técnicas y organizativas adecuadas para proteger los datos personales contra accesos no autorizados, pérdidas, alteraciones o destrucción. Además, la ley exige que los responsables informen a la Agencia de cualquier vulneración de seguridad que pueda poner en riesgo los derechos de los titulares.

(d) Deber de Protección desde el Diseño y por Defecto: Estas medidas deben estar integradas en el diseño de los sistemas y procesos de tratamiento de datos.

V. Tratamiento de datos por organismos públicos

Según lo establecido en el artículo 20 de la ley, los organismos públicos están autorizados para tratar datos personales sin necesidad de obtener el consentimiento del titular, siempre y cuando este tratamiento se realice en el marco de sus competencias legales y con la finalidad de cumplir con sus funciones específicas.

Para la consecución de estos fines, el Proyecto resalta la importancia de que estas entidades se rijan bajo los principios de coordinación, probidad y eficiencia, obligando a que los organismos públicos trabajen de manera articulada para evitar duplicidades y contradicciones en el tratamiento de datos personales.

VI. Normas de transferencia internacional de datos

La ley regula que la transferencia internacional de datos personales es lícita siempre que se cumplan los requisitos de autorización de tratamiento establecidos por la ley. Esta transferencia es permitida en los siguientes casos:

(a) Nivel adecuado de protección: Cuando el país de destino cuenta con un ordenamiento jurídico que proporciona niveles adecuados de protección de datos personales, similares a los establecidos en la legislación nacional.

(b) Cláusulas contractuales: Si la transferencia está respaldada por cláusulas contractuales que aseguren la protección adecuada de los datos personales durante su tratamiento en el extranjero.

(c) Mecanismos de cumplimiento y certificación: Cuando ambas partes involucradas en la transferencia tienen implementado un modelo de cumplimiento o mecanismo de certificación que ofrezca garantías adecuadas para la protección de los datos personales transferidos.

VII. Agencia de Protección de Datos Personales

Este nuevo órgano público, legalmente autónomo y con amplias atribuciones y funciones estará dirigido por un consejo directivo ("Consejo"). Así, la Agencia se posiciona como el órgano clave para garantizar la integridad y seguridad de la información personal en el país en virtud de sus facultades fiscalizadoras, interpretativas y sancionadoras.

(a) La Agencia es una corporación autónoma de derecho público, con personalidad jurídica y patrimonio propio, que opera de manera independiente y descentralizada. Su principal objetivo es velar por la efectiva protección de los derechos de los titulares de datos personales.

(b) La Agencia cuenta con diversas funciones y atribuciones, incluyendo:

- Potestad reglamentaria: Puede regular las operaciones de tratamiento de datos personales mediante normas específicas.
- Potestad interpretativa: Tiene la capacidad de interpretar las normas relacionadas con la protección de datos.
- Potestad sancionatoria: Está facultada para imponer sanciones en caso de infracciones a la ley.
- Resolución de solicitudes y reclamos: Atiende y resuelve las solicitudes y reclamos presentados por los titulares de datos.

- Difusión y educación: Desarrolla programas y acciones para la difusión y educación en temas de protección de datos.
- Certificación y supervisión: Certifica y supervisa modelos de prevención de infracciones, programas de cumplimiento y administra el Registro Nacional de Sanciones y Cumplimiento.

(c) Dirección de la Agencia: La dirección superior de la Agencia está a cargo del Consejo Directivo, compuesto por tres consejeros designados por el Presidente de la República con acuerdo del Senado. Sus principales funciones incluyen:

1. **Coordinación con el CPLT:** La Agencia debe coordinarse con el Consejo para la Transparencia (CPLT) cuando dicte una instrucción o norma de carácter general que pueda incidir en las competencias de dicho Consejo.
2. **Estatuto de los Funcionarios y Fiscalización:** La Agencia está sometida a la fiscalización de la Contraloría General de la República (CGR) y a las normas de probidad. Además, sus funcionarios estarán regidos por el Código del Trabajo.

VIII. Régimen de sanciones y responsabilidad civil

(i) Régimen de sanciones

La ley establece un marco de sanciones para asegurar el cumplimiento de sus disposiciones, clasificando las infracciones en leves, graves y gravísimas según la gravedad del incumplimiento. A continuación, señalamos algunos ejemplos de los distintos tipos de infracciones regulados por la ley.

- Infracción leve: Omitir la respuesta a las solicitudes del titular de datos.
- Infracción grave: Como el tratamiento de datos personales sin una base legal adecuada o para una finalidad distinta a la que fueron recolectados.
- Infracción gravísima: Se refiere al tratamiento de datos personales de forma fraudulenta.

(a) Las sanciones por infracciones varían según su gravedad:

- Infracciones leves: Se sancionan con una amonestación o una multa de hasta 5.000 UTM.
- Infracciones graves: Se castigan con multas que van desde 5.001 hasta 10.000 UTM.
- Infracciones gravísimas: Estas conlleven multas que oscilan entre 10.001 y 20.000 UTM.

En caso de reincidencia en infracciones graves o gravísimas, y respecto de empresas que no sean de menor tamaño, se puede imponer una sanción adicional que corresponde a un 2% a 4% de los ingresos anuales por ventas y servicios.

(b) Al fijar la multa, la Agencia deberá ponderar prudencialmente diversos factores:

- La gravedad de la conducta.
- Si la infracción fue cometida con falta de diligencia.
- El perjuicio causado.
- El beneficio económico obtenido.
- Si la infracción involucró datos personales sensibles o datos de menores de edad.
- La capacidad económica del infractor.

(c) En casos de infracciones gravísimas reiteradas dentro de un período de dos años, la Agencia tiene la facultad de suspender las operaciones y actividades de tratamiento de datos por un período de hasta 30 días.

(d) La Agencia mantendrá un Registro Nacional de Sanciones y Cumplimiento para garantizar la transparencia en la aplicación de las sanciones.

(e) Las acciones para sancionar infracciones prescriben a los 4 años desde que ocurrió el hecho.

(ii) Responsabilidad civil

El Proyecto establece un régimen de responsabilidad en contra de quienes hayan generado cualquier perjuicio económico directo o indirecto, así como el daño moral o psicológico sufrido por la persona afectada. El responsable deberá indemnizar tanto el daño patrimonial como el extrapatrimonial que se cause a los titulares de los datos.

Las acciones civiles para reclamar indemnización prescriben en un plazo de 5 años desde que se tuvo conocimiento del daño o de su manifestación.

IX. Modelo de prevención de infracciones

El Proyecto establece que una forma de prevenir infracciones a dicha normativa y evitar sanciones es a través la implementación de un modelo de prevención de infracciones. Este modelo no solo busca mitigar los riesgos asociados al tratamiento de datos, sino también fomentar una cultura de cumplimiento dentro de las empresas y organismos públicos.

(a) Programa de Cumplimiento Voluntario: Este programa debe ser incorporado como una obligación en los contratos de trabajo o de prestación de servicios, así como en el Reglamento Interno de las organizaciones, asegurando así su formalización y adopción efectiva.

(b) Delegado de Protección de Datos: deberá ser designado por la máxima autoridad directiva o administrativa responsable del tratamiento de datos. Este delegado, que puede ser nombrado tanto en organismos públicos como en empresas privadas, debe contar con autonomía para actuar en materias relacionadas con la protección de datos, independiente de la administración general.

(c) Funciones del Delegado:

- Informar y asesorar a los responsables de datos, a los encargados del tratamiento, y a los demás dependientes de la organización sobre las disposiciones de la ley.
- Promover y participar en la formulación de políticas de protección de datos dentro de la organización, asegurando que estas se alineen con los principios y normativas establecidas.
- Supervisar el cumplimiento de la ley, garantizando que todas las actividades de tratamiento de datos se realicen de acuerdo con los requerimientos legales.

(d) Certificación y Supervisión: La Agencia de Protección de Datos será la entidad encargada de certificar, registrar y supervisar que el modelo de prevención de infracciones cumpla con los requisitos y elementos establecidos por la ley y su reglamento. Esta certificación asegura que el modelo implementado sea efectivo y acorde a las mejores prácticas en protección de datos.