Observatorio de Consumidores en Políticas Públicas

Ley N°21.719 de Protección de Datos Personales

FONDO CONCURSABLE
Para Asociaciones de Consumidores

ODECU
ORGANIZACIÓN DE CONSUMIDORES Y USUARIOS

Ley N°21.719
de Protección de Datos Personales

Observatorio de Consumidores en Políticas Públicas

Contexto y antecedentes

La Ley 21.719, oficialmente la ley llamada "Regula la Protección y el Tratamiento de los Datos Personales y Crea la Agencia de Protección de Datos Personales", fue publicada el 13 de diciembre de 2024 y entrará en vigencia el 1 de diciembre de 2026 (Biblioteca del Congreso Nacional de Chile, 2024). Esta Ley, representa una modernización integral del marco normativo chileno en materia de protección de datos personales, reemplazando y modificando la antigua Ley N° 19.628 que había quedado obsoleta frente a los desafíos tecnológicos actuales (Piranha Risk, 2025). Esta nueva legislación busca alinear Chile con estándares internacionales de protección de datos, tomando como referencia el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, aunque adaptándose a la realidad nacional.

El proceso legislativo de esta ley fue extenso, fueron aproximadamente 7 años desde su presentación inicial hasta su publicación final, con diversas discusiones en el intertanto. Además, durante este período se realizaron múltiples consultas tanto con expertos, como organizaciones de la sociedad civil y el sector privado para lograr un equilibrio entre la protección efectiva de los datos personales y la viabilidad práctica de su implementación en el contexto y condiciones chilenas.

Esta nueva ley tiene como propósito fundamental regular la forma y condiciones en las que se realiza el tratamiento de datos personales en Chile, buscando mejorar significativamente la protección de los derechos de los titulares de datos (Gobierno de Chile, 2024). La finalidad de esta ley es crear un marco normativo integral que garantice el derecho a la privacidad en la era digital, para lo cual establece una autoridad supervisora especializada que será la Agencia de Protección de Datos Personales.

Asimismo, la legislación procura actualizar completamente el marco legal vigente, adaptándolo a los desafíos tecnológicos contemporáneos como el big data, la inteligencia artificial, el internet de las cosas y las nuevas y diversas formas que existen de procesamiento automatizado de información personal. Este enfoque prospectivo busca que la ley mantenga su relevancia ante futuros desarrollos y avances tecnológicos.

Una de las innovaciones más importantes de la Ley 21.719 es la creación de la Agencia de Protección de Datos Personales, esta será una entidad autónoma de derecho público con carácter técnico y descentralizado (Idónea, 2025). Esta agencia tendrá personalidad jurídica y patrimonio propio, relacionándose con el Presidente de la República a través del Ministerio de Justicia y Derechos Humanos.

La Agencia tendrá amplias facultades, entre las cuales se encuentran la supervisión, investigación y sanción en materia de protección de datos personales. En cuanto a las atribuciones en términos reguladores y penalizadores se incluye la capacidad de imponer multas significativas por incumplimientos, realizar investigaciones de oficio o por denuncias. También, puede emitir instrucciones y guías técnicas, y supervisar el cumplimiento de la ley tanto en el sector público como privado. Su creación responde a la necesidad de contar con una autoridad especializada que pueda enfrentar la complejidad técnica y jurídica de la protección de datos en el siglo XXI.

Ámbitos de aplicación y principales cambios

La Ley 21.719 tiene un ámbito de aplicación amplio que incluye a personas naturales que realicen tratamiento de datos personales, personas jurídicas del sector privado, y organismos públicos en todos sus niveles administrativos. Esta cobertura integral asegura que tanto el sector público como el privado estarán sujetos a las mismas obligaciones básicas de protección de datos, aunque con algunas especificidades según el contexto.

En términos territoriales, la ley tiene aplicación tanto a nivel nacional como a tratamientos transfronterizos que afecten a personas residentes en Chile. Esto significa que empresas extranjeras que procesen datos de personas en Chile también estarán sujetas a esta legislación, siguiendo el modelo del RGPD europeo que establece criterios de aplicación extraterritorial, pues la intención es resguardar los datos de todos los chilenos, independiente de quienes sean los que los manejen.

El sistema sancionatorio representa uno de los cambios más significativos de la nueva ley (Prelafit Compliance, 2024). Las multas son variables según la gravedad de la infracción y pueden alcanzar hasta 20.000 UTM, lo que equivale aproximadamente a $1,39 millones de dólares al momento de la publicación de la ley. Este régimen sancionatorio se complementa con un Registro Nacional de Sanciones y Cumplimiento que puede afectar significativamente la reputación empresarial y las oportunidades comerciales de las organizaciones infractoras.

La nueva legislación fortalece considerablemente los derechos de las personas sobre sus datos personales, estableciendo un catálogo amplio que incluye el derecho de acceso, rectificación, eliminación, portabilidad y oposición al tratamiento. Estos derechos van más allá de lo que contemplaba la legislación anterior y se alinean con estándares internacionales modernos de protección de datos.

La ley también incorpora un modelo de prevención de infracciones que incentiva a las organizaciones a implementar programas internos de prevención de infracciones en materia de protección de datos (Extend, 2024). Este enfoque preventivo busca que las organizaciones adopten una cultura de protección de datos desde el diseño y por defecto, reduciendo la probabilidad de incumplimientos y mejorando la protección efectiva de la información personal.

El período entre la publicación de la ley y su entrada en vigencia (desde diciembre 2024 hasta diciembre 2026) constituye una fase de preparación y adaptación crucial. Durante este tiempo, se espera que se desarrolle completamente la institucionalidad de la Agencia de Protección de Datos Personales, incluyendo la contratación de personal especializado, el desarrollo de reglamentos complementarios y la creación de sistemas informáticos necesarios para su operación.

Las organizaciones públicas y privadas también deben utilizar este período para adaptar sus procesos, sistemas y políticas internas a los nuevos requerimientos legales. La entrada en vigencia plena el 1 de diciembre de 2026 marca el momento en que la Agencia comenzará sus operaciones completas y se podrán aplicar las sanciones establecidas en la ley.

Asimismo, las organizaciones deberán implementar medidas técnicas y organizativas adecuadas para la protección de datos personales, estableciendo bases legales claras para todo tratamiento de datos que realicen. Deberán garantizar el ejercicio efectivo de los derechos de los titulares de datos, lo que implica crear procedimientos y sistemas que permitan a las personas acceder, corregir, eliminar o transferir sus datos de manera eficiente y que los dueños de sus datos consientan para cualquier tipo de estos movimientos que se hagan respecto de sus datos.

La obligación de notificar brechas de seguridad cuando corresponda representa otro cambio significativo, requiriendo que las organizaciones implementen sistemas de detección y respuesta ante incidentes de seguridad. Además, deberán mantener registros detallados de sus actividades de tratamiento y, en ciertos casos, designar responsables específicos de protección de datos dentro de su estructura organizacional.

Los sectores más impactados incluyen servicios financieros, comercio electrónico, telecomunicaciones, salud, educación y el sector público en general. Estos sectores manejan grandes volúmenes de datos personales sensibles y deberán realizar ajustes significativos en sus operaciones para cumplir con los nuevos estándares de protección.

Aspectos técnicos relevantes

La ley establece principios estrictos para el tratamiento de datos personales que incluyen licitud y transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación, integridad y confidencialidad. Estos principios deben guiar todas las decisiones relacionadas con el procesamiento de información personal, desde el diseño de sistemas hasta la definición de políticas corporativas.

Las organizaciones deberán implementar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo que presenta el tratamiento de datos. Esto incluye tanto medidas tecnológicas como pseudonimización, cifrado y controles de acceso, así como medidas organizativas como capacitación del personal, políticas internas y procedimientos de respuesta ante incidentes.

En el contexto de los nuevos derechos establecidos por la ley, herramientas como el "Rutificador" que permite a las personas eliminar sus datos de ciertos sistemas adquieren especial relevancia. Este tipo de herramientas se alinea perfectamente con el derecho de eliminación o "derecho al olvido" establecido en la nueva legislación, facilitando el ejercicio práctico de este derecho por parte de los ciudadanos.

En general, las organizaciones privadas deben comenzar inmediatamente con una auditoría completa de los datos personales que procesan, identificando qué información manejan, con qué propósitos, bajo qué bases legales y durante cuánto tiempo. Deben desarrollar o actualizar sus políticas de privacidad, capacitar a su personal en los nuevos requerimientos, evaluar y mejorar sus medidas de seguridad, y considerar la designación de un Oficial de Protección de Datos.

Los organismos públicos enfrentan desafíos similares pero con particularidades propias del sector público. Deben revisar su normativa interna para adaptarla a los nuevos requerimientos, mejorar la transparencia sobre el tratamiento de datos ciudadanos, asegurar que sus sistemas de intercambio de información cumplan con la nueva ley, y establecer mecanismos eficientes para que los ciudadanos puedan ejercer sus derechos.

Perspectiva comparada

- El Modelo Europeo: RGPD como Referencia Global

La Ley 21.719 chilena sigue claramente el modelo establecido por el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, que entró en vigor el 25 de mayo de 2018 y se ha convertido en el estándar de facto para la protección de datos a nivel mundial (Enríquez, 2020). El RGPD provocó que varios países latinoamericanos reformaran y actualizaran su legislación local sobre protección de datos personales, estableciendo un efecto dominó que ha influenciado la legislación de protección de datos en todo el mundo (Banco Interamericano de Desarrollo, 2022) y en Chile no fue la excepción.

Las similitudes entre la Ley 21.719 y el RGPD son evidentes en varios aspectos fundamentales. Ambas legislaciones establecen principios similares para el tratamiento de datos personales, incluyendo licitud, transparencia, limitación de la finalidad y minimización de datos. Los derechos de los titulares también siguen patrones similares, incluyendo derechos de acceso, rectificación, eliminación y portabilidad de datos. El régimen sancionatorio de Chile, con multas que pueden alcanzar 20.000 UTM, se inspira en el modelo europeo que permite multas de hasta el 4% del volumen de negocios anual global.

Sin embargo, la ley chilena presenta adaptaciones al contexto nacional que la distinguen del modelo europeo. Por ejemplo, en cuanto al plazo de entrada en vigencia de dos años (comparado con los dos años que también tuvo el RGPD desde su aprobación) permite una implementación más gradual, mientras que la creación de una agencia completamente nueva refleja la realidad institucional chilena, a diferencia de Europa donde ya existían autoridades de protección de datos en cada país miembro.

- América Latina: Un Panorama Heterogéneo

El contexto latinoamericano presenta un panorama muy diverso en materia de protección de datos personales (Asociación por los Derechos Civiles, 2016). Argentina fue el primer país en establecer una normativa para la protección de datos personales en 2000, siguiendo el modelo europeo, con la Ley N° 25.326, pero esta legislación ha mostrado limitaciones significativas en el contexto digital actual.

Colombia es el país que tiene la legislación sobre protección de datos más desarrollada en América Latina, con leyes que están vigentes desde 2012 (Garrigues, 2023). La Ley 1.581 estableció un marco robusto que incluye una autoridad independiente (la Superintendencia de Industria y Comercio) y un régimen sancionatorio que permite penalidades anuales del 2% de las ganancias por incumplimiento de la protección de datos.

Brasil representa otro caso destacado con la Lei Geral de Proteção de Dados (LGPD), que entró en vigor en 2020 y establece un marco muy similar al RGPD europeo (Mailjet, 2022). Por otro lado, México cuenta con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares desde 2010, aunque con un enfoque más limitado que las legislaciones más recientes.

Posicionamiento de Chile en el Contexto Regional

La nueva Ley 21.719 posicionará a Chile como uno de los países con legislación más avanzada en la región, superando en varios aspectos a legislaciones más antiguas como la argentina o la mexicana. El modelo chileno se distingue por varios elementos innovadores: la creación de una agencia completamente nueva y especializada, un régimen sancionatorio robusto que incluye multas significativas, y un catálogo amplio de derechos para los titulares de datos que incluye derechos modernos como la portabilidad de datos.

Comparado con pares regionales, el período de implementación de dos años de Chile proporciona una ventaja significativa sobre países que implementaron sus leyes con períodos de transición más cortos. Esto permite una mejor preparación tanto de las instituciones regulatorias como del cumplimiento del sector privado. La naturaleza especializada de la Agencia de Protección de Datos también distingue a Chile de países donde la supervisión de protección de datos es manejada por organismos regulatorios existentes con mandatos más amplios.

En contraste con el modelo europeo que Chile ha adoptado, los países anglosajones presentan enfoques diferentes. La protección de datos en Estados Unidos es diferente a la europea, con un enfoque sectorial y fragmentado que incluye leyes específicas para diferentes industrias (HIPAA para salud, GLBA para servicios financieros, COPPA para menores) pero sin una ley federal comprehensiva.

Estados Unidos mantiene este enfoque sectorial sin una regulación integral, lo que contrasta con la decisión de Chile de adoptar un enfoque integral similar al europeo. Esta elección proporcionará mayor certeza jurídica y protección uniforme en todos los sectores de la economía chilena.

La adopción del modelo europeo por parte de Chile tiene implicaciones importantes para las transferencias internacionales de datos. La Comisión Europea ha declarado como países con nivel adecuado de protección a un número limitado de países, y Chile podría aspirar a obtener esta declaración de adecuación una vez que su ley esté completamente implementada.

Esta declaración de adecuación sería significativa para las empresas chilenas que operan internacionalmente, ya que facilitaría enormemente las transferencias de datos con Europa sin necesidad de medidas adicionales de protección. Esto representaría una ventaja competitiva importante en el comercio digital internacional.

Conclusiones

Sin lugar a dudas, la Ley 21.719 representa un avance significativo y necesario en la protección de datos personales en Chile, elevando los estándares nacionales a nivel internacional y proporcionando herramientas efectivas para la protección de la privacidad en la era digital. Su implementación requerirá un esfuerzo considerable y sostenido por parte de organizaciones públicas y privadas, pero establecerá un marco sólido y moderno para enfrentar los desafíos actuales y futuros de la protección de datos.

Desde una perspectiva comparada, Chile ha tomado una decisión estratégica acertada al adoptar el modelo europeo de protección de datos, posicionándose en la vanguardia regional junto con países como Colombia y Brasil. Esta decisión contrasta favorablemente con países que mantienen legislaciones obsoletas o fragmentadas, como Argentina con su ley del año 2000 o México con un enfoque más limitado.

La adopción del estándar europeo coloca a Chile en una posición privilegiada para obtener una eventual declaración de adecuación por parte de la Unión Europea, lo que facilitaría enormemente el comercio digital internacional y las transferencias de datos con el bloque europeo. Esta ventaja competitiva podría ser determinante para empresas chilenas que buscan expandirse internacionalmente o para atraer inversión extranjera en sectores intensivos en datos.

El modelo chileno presenta ventajas distintivas incluso comparado con referentes regionales como Colombia. La creación de una agencia completamente nueva y especializada, en lugar de asignar estas funciones a una superintendencia existente, permite un enfoque más técnico y especializado. El régimen sancionatorio, con multas que pueden alcanzar niveles significativos, establece incentivos reales para el cumplimiento, superando las limitaciones de legislaciones con sanciones menos disuasivas.

La experiencia internacional demuestra que el éxito de una ley de protección de datos no depende únicamente de su calidad normativa, sino también de la efectividad de su implementación y supervisión. El caso del RGPD europeo muestra que una ley ambiciosa puede transformar las prácticas empresariales globales y establecer nuevos estándares de facto, pero también evidencia los desafíos de coordinación entre múltiples autoridades nacionales.

Chile tiene la oportunidad de aprender de estas experiencias internacionales. La decisión de crear una sola agencia nacional evita los problemas de coordinación que ha enfrentado Europa, mientras que el período de implementación de dos años permite una preparación más cuidadosa que países que implementaron cambios abruptamente.

La vigencia diferida hasta diciembre de 2026 proporciona un período de gracia valioso para la preparación, pero las organizaciones no deben subestimar la complejidad de los cambios requeridos. La experiencia internacional sugiere que las organizaciones que comiencen temprano sus procesos de adaptación estarán mejor posicionadas para cumplir oportunamente con los nuevos requerimientos y aprovechar las ventajas competitivas que puede proporcionar un manejo responsable y transparente de los datos personales.

El contexto comparativo también revela que Chile tiene la oportunidad de convertirse en un hub digital regional, aprovechando su marco normativo avanzado para atraer empresas que buscan operar bajo estándares internacionales de protección de datos. Esto podría ser particularmente relevante para sectores como fintech, servicios digitales y comercio electrónico.

El éxito de esta nueva legislación dependerá no solo de la efectividad de la Agencia de Protección de Datos Personales, sino también del compromiso de las organizaciones y la conciencia de los ciudadanos sobre sus derechos. La protección de datos personales es una responsabilidad compartida que requiere la participación activa de todos los actores del ecosistema digital chileno.

La perspectiva comparada internacional demuestra que Chile ha tomado decisiones acertadas en el diseño de su marco normativo, posicionándose como líder regional en protección de datos personales. Sin embargo, el verdadero test será la implementación efectiva de la ley y la capacidad de la nueva agencia para supervisar y hacer cumplir estos estándares elevados. La experiencia de otros países sugiere que el éxito en esta etapa será determinante para consolidar a Chile como referente en la materia y aprovechar las ventajas competitivas que ofrece un marco robusto de protección de datos en la economía digital global.

Preguntas guía para la discusión

1. Implementación y Preparación Institucional

- ¿Es suficiente el período de preparación de dos años (2024-2026) para que las organizaciones públicas y privadas se adapten completamente a los nuevos requerimientos? Considere las diferencias entre sectores altamente digitalizados y aquellos más tradicionales.
- ¿Qué desafíos específicos enfrentará la nueva Agencia de Protección de Datos Personales en sus primeros años de operación? ¿Cómo puede asegurar una implementación efectiva sin generar disrupciones innecesarias en el mercado?
- ¿Cuáles deberían ser las prioridades de la Agencia durante el período de transición? ¿Debería enfocarse más en educación y orientación o en fiscalización y sanción?

2. Impacto Económico y Competitividad

- ¿Cómo afectará el alto nivel de multas (hasta 20.000 UTM) a las PYMES chilenas versus las grandes corporaciones? ¿Existe riesgo de crear barreras de entrada desproporcionadas para empresas más pequeñas?
- ¿Qué sectores de la economía chilena podrían beneficiarse más de tener un marco robusto de protección de datos? ¿Cómo puede esto convertirse en una ventaja competitiva internacional?
- ¿La implementación de esta ley podría acelerar la digitalización de sectores tradicionales de la economía chilena? ¿Cuáles serían las consecuencias positivas y negativas de este proceso?

3. Perspectiva Comparada Regional

- ¿Debería Chile aspirar a obtener una declaración de adecuación de la Unión Europea? ¿Cuáles serían los beneficios y costos de este reconocimiento?
- ¿Cómo puede Chile aprovechar su posición de liderazgo regional en protección de datos para atraer inversión extranjera y desarrollar un ecosistema digital robusto?
- ¿Qué lecciones específicas puede aprender Chile de la experiencia de implementación del RGPD en Europa y de la LGPD en Brasil?

4. Derechos Ciudadanos y Cultura Digital

- ¿Están los ciudadanos chilenos suficientemente informados sobre sus nuevos derechos digitales? ¿Qué estrategias de educación ciudadana serían más efectivas?
- ¿Cómo puede garantizarse que el ejercicio de derechos como la portabilidad de datos no se convierta en una carga burocrática excesiva tanto para ciudadanos como para organizaciones?
- ¿Qué rol deberían jugar las organizaciones de la sociedad civil en la supervisión de la implementación de esta ley?

5. Desafíos Tecnológicos y Futuros

- ¿Está la ley suficientemente preparada para enfrentar desafíos tecnológicos emergentes como la inteligencia artificial generativa, el metaverso y la computación cuántica?
- ¿Cómo puede la Agencia de Protección de Datos mantenerse actualizada frente al rápido avance tecnológico sin crear incertidumbre regulatoria?
- ¿Qué medidas específicas deberían implementarse para proteger datos sensibles en sectores críticos como salud y servicios financieros?

6. Evaluación Crítica del Modelo Adoptado

- ¿Fue acertada la decisión de crear una agencia completamente nueva en lugar de fortalecer instituciones existentes? Compare las ventajas y desventajas de ambos enfoques.
- ¿El modelo de prevención de infracciones (compliance) incluido en la ley es suficientemente robusto para incentivar el cumplimiento proactivo?
- ¿Existe riesgo de que el modelo sancionatorio sea demasiado severo y genere un efecto inhibidor en la innovación digital?

7. Sostenibilidad y Evolución a Largo Plazo

- ¿Cómo puede asegurarse que la ley mantenga su relevancia y efectividad en un con texto tecnológico que evoluciona rápidamente?
- ¿Qué mecanismos de evaluación y actualización periódica deberían implementarse para perfeccionar la aplicación de la ley basándose en la experiencia práctica?
- ¿Cuáles son los indicadores clave que deberían monitorearse para evaluar el éxito de la implementación de esta legislación en los próximos 5-10 años?

Referencias Bibliográficas

- Asociación por los Derechos Civiles. (2016). El sistema de protección de datos personales en América Latina (Vol. I). https://adc.org.ar/wp-content/uploads/2019/06/023-A-El-sistema-de-protecci%C3%B3n-de-datos-personales-en-Am%C3%A9rica-Latina-Vol.-I-12-2016.pdf
- Banco Interamericano de Desarrollo. (2022, 13 de julio). Despuntan las reformas en materia de protección de datos en América Latina. Abierto al público. https://blogs.iadb.org/conocimiento-abierto/es/proteccion-de-datos-gdpr-america-latina/
- Biblioteca del Congreso Nacional de Chile. (2024). Ley 21719: Regula la protección y el tratamiento de los datos personales y crea la agencia de protección de datos personales. https://www.bcn.cl/leychile/navegar?idNorma=1209272
- Enríquez, L. (2020). La visión de América Latina sobre el Reglamento General de Protección de Datos. Comentario Internacional: Revista del Centro Andino de Estudios Internacionales. https://repositorio.uasb.edu.ec/bitstream/10644/7704/1/07-CO-Enriquez.pdf
- Extend. (2024, 17 de diciembre). Nueva Ley de Protección de Datos Personales (Ley N° 21.719) Diciembre 2024. https://www.extend.cl/proyecto-de-ley-de-proteccion-de-datos-personales-bol-n-21-719-diciembre-2024/
- Garrigues. (2023, 27 de junio). ¿Cómo se regula la protección de datos en Latinoamérica y cómo influye el RGPD? https://www.garrigues.com/es_ES/noticia/regula-proteccion-datos-latinoamerica-influye-rgpd
- Gobierno de Chile. (2024, 27 de agosto). Aprobada Ley de Protección de Datos: ¿De qué trata? https://www.gob.cl/noticias/ley-proteccion-datos-personales-aprobacion-eleva-estandar-derechos/
- Idónea. (2025, 9 de marzo). Ley sobre Protección de los Datos Personales en Chile: Todo lo que Necesitas Saber (Guía Actualizada). https://idonea.cl/3181-2/
- Mailjet. (2022, 8 de septiembre). Protección de datos en Latinoamérica: Leyes que conocer. https://www.mailjet.com/es/blog/emailing/proteccion-datos-latinoamerica/
- Piranha Risk. (2025, 5 de febrero). Conoce la nueva Ley de protección de datos personales de Chile. https://www.piranirisk.com/es/blog/nueva-ley-proteccion-datos-chile
- Prelafit Compliance. (2024, 14 de diciembre). Ley 21719 Protección Datos Personales. https://prelafit.cl/ley-21719-proteccion-datos-personales/

ODECU

ORGANIZACIÓN DE CONSUMIDORES Y USUARIOS

FONDO CONCURSABLE
Para Asociaciones de Consumidores

Observatorio de Consumidores en Políticas Públicas