

**Descripción y síntesis de 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**

Serie Informes N° 12-25, 08-04-2025

*por Víctor Soto Martínez*

**Resumen**

*Se describen los elementos centrales de 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, y se realizan diversos comentarios generales a la institucionalidad y la normativa que allí se establece.*

Disclaimer: Este trabajo ha sido elaborado a solicitud de parlamentarios del Congreso Nacional, bajo sus orientaciones y particulares requerimientos. Por consiguiente, sus contenidos están delimitados por los plazos de entrega que se establezcan y por los parámetros de análisis acordados. No es un documento académico y se enmarca en criterios de neutralidad e imparcialidad política.

## TABLA DE CONTENIDOS

Antecedentes .....	3
1. Tramitación legislativa y descripción general .....	3
2. Objeto de la ley .....	4
3. Definiciones .....	4
4. Principios .....	5
5. Derechos .....	6
6. Tratamiento de los datos personales .....	7
7. Categorías especiales de datos .....	8
8. Tratamiento de datos personales por órganos públicos .....	8
9. Transferencia internacional de datos personales .....	8
10. Agencia de Protección de Datos Personales .....	9
11. Infracciones y sanciones .....	11
12. Procedimientos .....	12
13. Responsabilidad civil.....	12
14. Casos especiales: Poder Judicial, Congreso Nacional y otros .....	13
15. Disposiciones transitorias .....	13
Comentario general .....	14

## Antecedentes

Se ha solicitado un documento que sintetice y explique la nueva legislación chilena en materia de protección de datos personales, para apoyar la participación de la delegación del Congreso Nacional que asistirá a la próxima reunión de la *Comisión de Servicios Públicos y Defensa del Usuario y el Consumidor*, del Parlamento Latinoamericano (Parlatino), a realizarse los días 10 y 11 de abril.

Para ello, el presente informe se compone de una descripción general de cada elemento de la ley N° 21.719, incluyendo un relato breve de su tramitación legislativa, seguida de un comentario general sobre las innovaciones introducidas y su relación con otros modelos de protección de los datos personales a nivel internacional.

### 1. Tramitación legislativa y descripción general

La ley se originó como mensaje del Presidente de la República (boletín N° 11.144-07), y fue ingresado al Senado el 15 de marzo de 2017. Pronto fue refundido con una moción parlamentaria que también buscaba modificar la institucionalidad de protección de datos (boletín N° 11.092-07)<sup>1</sup>. Luego de una extensa discusión, el proyecto se aprobó en particular el 25 de enero de 2022.

En la Cámara de Diputados, en tanto, se aprobó con modificaciones el 8 de mayo de 2023. En el tercer trámite constitucional, ante el Senado, se rechazaron las modificaciones introducidas en la Cámara, lo que motivó la conformación de una comisión mixta el 4 de enero de 2024, cuyo informe fue aprobado el 27 de agosto de dicho año. Finalmente, la ley fue promulgada el 25 de noviembre de 2024 y publicada en el Diario Oficial el 13 de diciembre de dicho año.

La ley se presenta como una modificación de la ley N° 19.628, pero en la práctica reemplaza casi todos sus artículos, excepto: literales b), d), e) y k), que pasó a ser j), del art. 2°; arts. 17, 18 y 19 (aunque varios elementos de este último artículo también fueron modificados); y el primer inciso del artículo primero transitorio (los otros incisos se eliminaron). En este sentido, si bien la ley de protección de datos se seguirá identificando como "ley N° 19.628", lo cierto es que estamos frente a una nueva legislación.

Otro punto a relevar es que su entrada en vigencia ha quedado diferida hasta el mes de diciembre de 2026, por lo que en el intertanto seguirá operando la antigua ley N° 19.628.

En cuanto al fondo, la ley incorpora nuevos principios, como el principio de finalidad, el principio de seguridad o el de confidencialidad, entre otros.

---

<sup>1</sup> Moción firmada por los senadores Pedro Araya Guerrero, Alfonso De Urresti Longton, Felipe Harboe Bascuñán, Alberto Espina Otero y Hernán Larraín Fernández.

También se incorporan derechos, en particular el derecho de acceso a los datos y a conocer detalles de su tratamiento, el derecho de rectificación de los datos que sean inexactos, desactualizados o incompletos, el derecho de supresión de los datos, el derecho de oposición a algún tratamiento específico de estos, el derecho al bloqueo del tratamiento y el derecho a la portabilidad.

Asimismo, se regulan en detalle los deberes de los responsables del tratamiento de los datos, tanto personales como sensibles, y se establece un robusto sistema de infracciones y sanciones.

Para fiscalizar todos estos puntos, se crea una nueva gobernanza, dirigida por una Agencia de Protección de Datos Personales, que además tendrá a su cargo la dictación de instrucciones y la asesoría del gobierno respecto de la política de datos, entre otras funciones.

## **2. Objeto de la ley (art. 1°)**

Su principal objeto es **regular la forma y condiciones en las cuales se efectúa el tratamiento y protección de los datos personales de las personas naturales**, en conformidad al artículo 19, N° 4, de la Constitución (derecho al respeto y protección de la vida privada, a la honra de persona y su familia, y de sus datos personales). Para ello, se establece un régimen de tratamiento y protección de datos, del cual se excluye al tratamiento de datos que se realice en el ejercicio de las libertades de emitir opinión y de informar reguladas por las leyes a que se refiere el artículo 19, N° 12, de la Constitución (medios de comunicación), así como el tratamiento de datos que efectúen las personas naturales en relación con sus actividades personales (por ejemplo, en sus redes sociales).

Por otro lado, el art. 1° bis define su ámbito de aplicación territorial. Así, la ley es aplicable cuando: i) el responsable o mandatario de una empresa u organización esté establecido o constituido en el territorio nacional; ii) cuando dicho responsable realice las operaciones de tratamiento de datos personales a nombre de un responsable establecido o constituido en el territorio nacional; iii) cuando éste no se encuentre establecido en el territorio nacional pero sus operaciones de tratamiento de datos personales estén destinadas a ofrecer bienes o servicios a titulares que se encuentren en Chile; ó iv) cuando le resulte aplicable la legislación nacional a causa de un contrato o del derecho internacional.

## **3. Definiciones (art. 2°)**

Se establecen diversas definiciones clave, que modifican o amplían los conceptos establecidos por la ley N° 19.628. Así, entre otras cosas, se modifica el concepto de "dato personal", que pasa a ser definido como **"cualquier información vinculada o referida a una persona natural identificada o identificable"**. Se considerará

identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante uno o más identificadores, tales como el nombre, el número de cédula de identidad, el análisis de elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona" (letra f).

También se incorpora el concepto de "datos personal sensible", es decir, aquel dato referido "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" (letra g).

Por otro lado, se incorporan conceptos tales como "anonimización" y "seudonimización", siendo el primero 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" (letra k) y el segundo un "tratamiento de datos personales que se efectúa de manera tal que ya no puedan atribuirse a un titular sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona natural identificada o identificable" (letra l).

Para efectos de la comprensión de la ley, es muy relevante la definición del **responsable** de datos, es decir, "toda persona natural o jurídica, pública o privada, que decide acerca de los fines y medios del tratamiento de datos personales, con independencia de si los datos son tratados directamente por ella o a través de un tercero mandatario o encargado" (letra n). Lo mismo vale para el **titular** de datos, es decir, la "persona natural, identificada o identificable, a quien conciernen o se refieren los datos personales" (letra ñ).

#### 4. Principios (art. 3°)

La ley define nuevos principios (ocho en total), de los cuales destacaremos los que nos parecen más relevantes. Así, se establecen el **principio de finalidad** (letra b), según el cual los datos personales deben ser recolectados con fines específicos, explícitos y lícitos, y el **principio de proporcionalidad** (letra c), según el cual los datos personales que se traten deben limitarse estrictamente a aquéllos que resulten necesarios, adecuados y pertinentes en relación con los fines del tratamiento.

Como contrapartida, se incorpora también un **principio de responsabilidad** (letra e), que dispone que quienes realicen tratamiento de los datos personales serán legalmente responsables del cumplimiento de los principios contenidos en este artículo

y de las obligaciones y deberes de conformidad a la ley. También un **principio de seguridad** (letra f), que obliga al responsable a garantizar estándares adecuados de seguridad, protegiendo los datos contra el tratamiento no autorizado o ilícito, y contra su pérdida, filtración, daño accidental o destrucción.

Por otro lado, según el **principio de confidencialidad** (letra h), el responsable de datos personales y quienes tengan acceso a ellos deberán guardar secreto o confidencialidad acerca de los mismos, disponiendo de medidas adecuadas para ello. Cabe mencionar que este es un deber que subsiste aún después de concluida la relación con el titular.

## 5. Derechos (arts. 4 al 11)

La ley incluye diversos derechos nuevos para el titular de derechos personales. Así, se establece:

-**Derecho de acceso** (art. 5): el derecho del titular de datos a solicitar y obtener del responsable, confirmación acerca de si sus datos personales están siendo tratados por él, acceder a ellos en su caso, y a la información prevista en esta ley;

-**Derecho de rectificación** (art. 6): el derecho del titular de datos a solicitar y obtener del responsable, que modifique o complete sus datos personales, cuando están siendo tratados por él, y sean inexactos, desactualizados o incompletos;

-**Derecho de supresión** (art. 7): el derecho del titular de solicitar y obtener del responsable que suprima o elimine sus datos personales, de acuerdo a las causales previstas en la ley;

-**Derecho de oposición** (art. 8): derecho a solicitar y obtener del responsable, que no se lleve a cabo un tratamiento de datos determinado, de conformidad a las causales previstas en la ley;

-**Derecho de bloqueo del tratamiento** (art. 8 ter): el titular de datos tiene derecho a solicitar la suspensión temporal de cualquier operación de tratamiento de sus datos personales cuando formule una solicitud de rectificación, supresión u oposición, mientras dicha solicitud no se resuelva;

-**Derecho a la portabilidad** (art. 9), es decir, el derecho del titular de datos a solicitar y obtener del responsable, una copia de sus datos personales en un formato electrónico estructurado, genérico y de uso común, que permita ser operado por distintos sistemas, y poder comunicarlos o transferirlos a otro responsable de datos.

Para ejercer los primeros tres derechos indicados, el titular de los datos debe presentar una solicitud o requerimiento escrito ante el responsable, dirigido a la dirección de correo electrónico establecida para este fin, un formulario de contacto o un medio electrónico equivalente. Además de su individualización, la solicitud debe

identificar los datos respecto de los cuales está ejerciendo el derecho respectivo (rectificación, supresión u oposición). Aquí se inicia un pequeño procedimiento entre el titular y el responsable que, en caso de denegación total o parcial de la solicitud, puede desembocar en una reclamación del titular ante la Agencia de Protección de Datos Personales (art. 11, y véase también el art. 41).

## 6. Tratamiento de los datos personales (arts. 12 al 16 ter)

Por regla general es lícito el tratamiento de los datos personales que le conciernen al titular, cuando otorgue su **consentimiento** para ello. Este consentimiento debe ser **libre, informado y específico** en cuanto a su finalidad o finalidades, y manifestarse, además, **en forma previa y de manera inequívoca**, mediante una declaración **verbal, escrita o expresada a través de un medio electrónico equivalente**, o mediante un **acto afirmativo** que dé cuenta con claridad de la voluntad del titular (art. 12, inc. 1º y 2º). Además es **esencialmente revocable**, tanto así que, de acuerdo a la ley, los “medios utilizados para el otorgamiento o la revocación del consentimiento deben ser expeditos, fidedignos, gratuitos y estar permanentemente disponibles para el titular” (art. 12, inc. 5º).

Por otro lado, se presume que el consentimiento para tratar los datos no ha sido otorgado libremente “cuando el responsable lo recaba en el marco de la ejecución de un contrato o la prestación de un servicio en que no es necesario efectuar esa recolección” (art. 12, inc. 6º).

También hay una serie (taxativa) de hipótesis donde se podrá hacer tratamiento de datos sin el consentimiento del titular, como cuando el tratamiento sea necesario para la ejecución o el cumplimiento de una obligación legal o lo disponga la ley, cuando sea necesario para la celebración o ejecución de un contrato entre el titular y el responsable, o cuando sea necesario para la formulación, ejercicio o defensa de un derecho ante los tribunales de justicia u órganos públicos, entre otros (art. 13). Por cierto, en todos estos casos el responsable deberá acreditar la licitud del tratamiento.

Por lo demás, el responsable del tratamiento de los datos tiene una **serie de deberes** (art. 14 y ss.), entre los cuales destacan el **deber de secreto o confidencialidad** (art. 14 bis) y el **deber de información y transparencia** (art. 14 ter). En virtud de este último, por ejemplo, el responsable debe facilitar y mantener permanentemente a disposición del público, en su sitio web o en cualquier otro medio de información equivalente, informaciones tales como su política de tratamiento de datos personales, las categorías, clases o tipos de datos que trata; los destinatarios a los que se prevé comunicar o ceder los datos; las finalidades de los tratamientos que realiza; sus políticas de seguridad para proteger las bases de datos, etcétera. Asimismo, tiene el **deber de adoptar medidas de seguridad** (art. 14 quinquies) y de **reportar las vulneraciones a estas medidas ante la Agencia** (art. 14 sexies). Otro deber interesante es el de realizar, previo al inicio de las operaciones del tratamiento de datos personales, una **evaluación de impacto**, cuando sea probable que el tipo de

tratamiento pueda producir un alto riesgo para los derechos de los titulares (art. 15 ter).

Cabe mencionar que se establecen ciertas reglas particulares para el tratamiento de los datos personales sensibles. Así, hay una norma general (art. 16), una norma relativa a este tipo de datos cuando se vinculen con la salud y el perfil biológico humano (art. 16 bis) y una norma específica sobre los datos biométricos (art. 16 ter).

## **7. Categorías especiales de datos (arts. 16 quáter al 19)**

Se establecen deberes especiales para el tratamiento de datos personales relativos a los niños, niñas y adolescentes (art. 16 quáter), así como para el tratamiento de datos personales con fines históricos, estadísticos, científicos y de estudios o investigaciones (art. 16 quinquies), datos de geolocalización (art. 16 sexies), y datos relativos a obligaciones de carácter financiero, bancario o comercial (arts. 17, 18 y 19).

## **8. Tratamiento de datos personales por órganos públicos (arts. 20 al 26)**

En el caso de los órganos públicos, la regla general de tratamiento de datos personales se invierte. Así, **se considera lícito el tratamiento de los datos personales que efectúan los órganos públicos cuando se realiza para el cumplimiento de sus funciones legales, dentro del ámbito de sus competencias, de conformidad a las normas establecidas en la ley.**

En dichas condiciones, los órganos públicos actúan como responsables de datos y **no requieren el consentimiento del titular** para tratar sus datos personales (art. 20). Por cierto, el titular de los datos podrá ejercer ante el órgano público los derechos de acceso, rectificación y oposición que le reconoce esta ley (art. 23). Cabe mencionar que las condiciones, modalidades e instrumentos para la comunicación o cesión de datos personales entre organismos públicos y con personas u organismos privados, se regularán a través de un **reglamento** expedido por el Ministerio Secretaría General de la Presidencia y suscrito por el Ministro de Hacienda y por el Ministro de Economía, Fomento y Turismo, previo informe de la Agencia (art. 26).

## **9. Transferencia internacional de datos personales (arts. 27 al 29)**

La regla general en esta materia dispone que, cumplidos los requisitos establecidos en esta ley para autorizar al tratamiento de los datos, **las operaciones de transferencia internacional de datos serán lícitas** siempre y cuando se cumplan las hipótesis dispuestas en el artículo 27, vinculadas todas ellas con el establecimiento de **garantías y niveles de protección suficientes** (art. 27). Sin embargo, el mismo artículo establece varias excepciones, en casos específicos.

Por otro lado, también se establecen las reglas para que la Agencia determine cuáles son los países cuyo ordenamiento jurídico posee niveles adecuados de protección de datos (art. 28). A la Agencia también le corresponderá fiscalizar estas transferencias de datos (art. 29).

## **10. Agencia de Protección de Datos Personales (arts. 30 al 32)**

Se crea una **autoridad de control** en materia de protección de datos personales llamada Agencia de Protección de Datos Personales. Como se podrá apreciar se le asignan funciones importantes, especialmente en materia de fiscalización.

### **10.1. Objeto y naturaleza jurídica (art. 30)**

Su objeto es **velar por la efectiva protección de los derechos** que garantizan la vida privada de las personas y sus datos personales, y **fiscalizar** el cumplimiento de las disposiciones establecidas en esta ley.

Es un **servicio público descentralizado**, con personalidad jurídica y patrimonio propio, que se relacionará con el Presidente de la República a través del **Ministerio de Economía, Fomento y Turismo**.

### **10.2. Funciones y atribuciones (art. 30 bis)**

En primer lugar, tiene **funciones normativas**, ya que le corresponde dictar instrucciones y normas generales y obligatorias para regular las operaciones de tratamiento de datos personales según los principios establecidos en esta ley (letra a). En la misma línea, aplica e interpreta administrativamente las disposiciones legales y reglamentarias en materia de protección de los datos personales (letra b). También puede proponer al Presidente de la República y al Congreso Nacional, en su caso, las normas legales y reglamentarias para asegurar a las personas la debida protección de sus datos personales (letra g).

En segundo lugar, tiene **funciones fiscalizadoras** respecto del cumplimiento de las normas de la ley y de sus reglamentos e instrucciones (letra c). También determina las infracciones e incumplimientos en que incurran quienes realicen tratamiento de datos personales (letra d).

Como complemento de lo anterior, cuenta con **funciones sancionadoras** sobre las personas naturales o jurídicas que traten datos personales con infracción a esta ley, sus reglamentos, así como a las instrucciones y normas generales que ella misma dicte (letra e).

Por otro lado, tiene la función de **resolver las solicitudes y reclamos** que formulen los titulares de datos en contra de quienes traten datos personales (letra f).

Asimismo, tiene la atribución de **colaborar con los órganos públicos en el diseño e implementación de políticas** y acciones destinadas a velar por la protección de los datos personales y su correcto tratamiento (letra j).

### 10.3. Estructura orgánica (arts. 30 ter al 30 nonies)

La **dirección superior** de la Agencia le corresponderá a un **Consejo Directivo** (art. 30 ter), integrado por **tres consejeros**, designados por el Presidente de la República, con acuerdo del Senado, adoptado por los dos tercios de sus miembros en ejercicio (art. 30 quáter).

Los consejeros durarán **seis años** en sus cargos, sin que puedan ser renovados por un nuevo período. Se trata, por lo demás, de cargos de **dedicación exclusiva** (tienen la obligación de reunirse, a lo menos, una vez por semana). El Consejo Directivo designará a su presidente y vicepresidente de entre sus miembros. Estos cargos durarán tres años. Cabe mencionar, además, que el Consejo adoptará sus decisiones por la mayoría de sus miembros y el quórum mínimo para sesionar es de dos consejeros (art. 30 quáter).

Los consejeros tienen un **mecanismo de remoción calificado**, ya que se requiere un pronunciamiento de la Corte Suprema, sobre la base de un número acotado de causales. Este pronunciamiento sólo puede ser requerido por el Presidente de la República o la Cámara de Diputados mediante acuerdo adoptado por simple mayoría, o a petición de quince diputados, por incapacidad, mal comportamiento o negligencia manifiesta en el ejercicio de sus funciones (art. 30 sexies). Asimismo, el Consejo puede determinar sus propios estatutos (es decir, sus normas de funcionamiento interno), previa aprobación mediante decreto supremo expedido a través del Ministerio de Economía, Fomento y Turismo (art. 30 octies). Estos elementos dan cuenta de una autonomía reforzada del servicio, sin llegar a ser calificable como una autonomía legal (estructura orgánica que caracteriza al Consejo para la Transparencia, al Instituto Nacional de Derechos Humanos y a la Defensoría de la Niñez).

Al **presidente** del Consejo Directivo le corresponde actuar como **jefe de servicio**, lo que contempla ejecutar los acuerdos del Consejo, representar legal, judicial y extrajudicialmente a la Agencia, suscribir sus diversos contratos y convenios, y encargarse de la contratación y desvinculación del personal, entre otras funciones (art. 30 nonies).

### 10.4. Estatuto del personal de la Agencia (art. 32)

El personal de la Agencia se regirá por el **Código del Trabajo**. Sin perjuicio de ello, se le aplicarán las normas de **probidad administrativa**. En cuanto a sus directivos, se les aplicarán las normas y procedimientos de la **Alta Dirección Pública** (ley N° 19.882).

En el resto de sus elementos, funciona como un servicio público normal, según las normas de administración financiera del Estado y sometidos a la fiscalización de la Contraloría General de la República. Sin embargo, el legislador **exime a sus resoluciones del trámite de toma de razón**. Esto también puede ser interpretado como un elemento de autonomía adicional para este servicio.

## 11. Infracciones y sanciones (arts. 33 al 40)

Las infracciones realizadas por responsables de tratamiento de datos a los principios del art. 3, así como al resto de los deberes que hemos indicado aquí, se califican como **infracciones leves, graves y gravísimas** (art. 34).

Las primeras se encuentran enumeradas en el art. 34 bis e incluyen el incumplimiento total o parcial del deber de información y transparencia.

Las segundas se regulan en el art. 34 ter e incluyen, por ejemplo, el tratamiento de los datos personales sin contar con el consentimiento del titular de datos o sin un antecedente o fundamento legal que otorgue licitud al tratamiento, o tratarlos con una finalidad distinta de aquélla para la cual fueron recolectados.

Finalmente, las infracciones gravísimas están reguladas en el art. 34 quáter y contemplan la acción de destinar maliciosamente los datos personales a una finalidad distinta de la consentida por el titular o prevista en la ley que autoriza su tratamiento, así como tratar, comunicar o ceder, a sabiendas, datos personales sensibles o datos personales de niños, niñas y adolescentes.

Las sanciones se regulan en el art. 35, como se puede ver en la siguiente tabla:

**Cuadro N° 1. Escala de sanciones**

Infracciones	Sanciones
Leves	Amonestación escrita o multa hasta 5.000 UTM
Graves	Multa hasta 10.000 UTM
Gravísimas	Multa hasta 20.000 UTM

Elaboración propia a partir de la ley

Si el infractor no implementa las medidas propuestas por la Agencia en un plazo de 60 días, se le impondrá un recargo de 50% a la multa. En caso de reincidencia, la Agencia podrá aplicar una multa de hasta tres veces el monto asignado a la infracción. Y en el caso de grandes empresas (es decir, aquéllas no definidas como empresas de menor tamaño en la ley N° 20.416), la multa podrá alcanzar hasta el 2% (si la infracción es grave) o 4% (si la infracción es gravísima) de los ingresos anuales por ventas y servicios y otras actividades del giro en el último año calendario.

La ley establece, por cierto, ciertas reglas para la determinación de las circunstancias agravantes y atenuantes de responsabilidad (art. 36) y del monto de las multas (art. 37).

Por otro lado, la Agencia administrará un registro público y electrónico, de acceso gratuito, denominado **Registro Nacional de Sanciones y Cumplimiento**, donde se consignarán los responsables de datos que hayan sido sancionados por infringir los derechos y obligaciones establecidos en esta ley.

## **12. Procedimientos (arts. 41 al 46)**

La ley establece una serie de procedimientos para que los titulares de datos personales puedan hacer efectivos sus derechos. En primer lugar, el **procedimiento administrativo de tutela de derechos** (art. 41). Aquí el titular de datos podrá reclamar ante la Agencia cuando el responsable le haya denegado una solicitud de rectificación, supresión u oposición, o no hubiere dado respuesta a dicha solicitud dentro de plazo (art. 11).

En segundo lugar, se contempla el **procedimiento administrativo por infracción de ley**, es decir, el procedimiento, instruido por la Agencia, para determinar las infracciones que cometan los responsables de datos por incumplimiento o vulneración de los principios establecidos en el artículo 3º, de los derechos y obligaciones establecidos en la ley y la aplicación de las sanciones correspondientes. Este procedimiento se puede iniciar de oficio o a petición de parte (art. 42).

Como contrapartida, la ley considera un **procedimiento de reclamación judicial** contra las resoluciones de la Agencia. Así, las personas naturales o jurídicas interesadas que estimen que un acto administrativo que paraliza el procedimiento, o una resolución final o de término emanado de la Agencia, sea ilegal, podrán deducir un reclamo de ilegalidad ante la Corte de Apelaciones de Santiago o la del lugar donde se encuentre domiciliado el reclamante, a elección de este último. Este reclamo debe interponerse dentro de los 15 días hábiles siguientes a la notificación de la resolución impugnada (art. 43).

## **13. Responsabilidad civil (arts. 47 al 53)**

La ley en comento establece que, por regla general, el responsable de datos deberá **indemnizar el daño patrimonial y extrapatrimonial** que cause al o los titulares, cuando en sus operaciones de tratamiento de datos infrinja los principios establecidos en el artículo 3º, los derechos y obligaciones establecidos en la ley y les cause perjuicio (art. 47).

Para prevenir este tipo de infracciones y daños, la ley establece que los responsables de datos podrán adoptar un **modelo de prevención de infracciones** consistente en un **programa de cumplimiento** (art. 49), el que será **certificado por la Agencia**, la que también incorporará en el Registro Nacional de Sanciones y Cumplimiento a las entidades que posean una certificación vigente (art. 51). Esta certificación durará tres años (art. 52).

Por otro lado, el responsable de datos podrá designar un **delegado de protección de datos personales**. Este será designado por la máxima autoridad directiva o administrativa del responsable de datos y deberá contar con autonomía respecto de la administración. Tendrá diversas funciones –además de las que les pudiera asignar el responsable de datos–, entre las cuales destacamos la función de informar y asesorar al responsable respecto de las disposiciones legales y reglamentarias relativas al derecho a la protección de los datos personales, así como supervisar su cumplimiento y actuar como punto de contacto de la Agencia (art. 50).

#### **14. Casos especiales: Poder Judicial, Congreso Nacional y otros (arts. 54 y 55)**

Se establece como regla general la **licitud del tratamiento de los datos personales que efectúan el Congreso Nacional, el Poder Judicial, la Contraloría General de la República, el Ministerio Público, el Tribunal Constitucional, el Banco Central, el Servicio Electoral y la Justicia Electoral, y los demás tribunales especiales creados por ley**, cuando se realiza para el cumplimiento de sus funciones legales, dentro del ámbito de sus competencias y, de conformidad a las normas especiales que se establecen en sus respectivas leyes orgánicas, así como las normas aplicables a los órganos públicos en esta ley (art. 20 y ss), excepto en lo referido a la intervención de la Contraloría General de la República en la determinación de la responsabilidad administrativa y en la aplicación de la ley N° 18.834. Por otra parte, los funcionarios de estos organismos deben guardar secreto de tales datos. En esas condiciones estas instituciones y organismos tienen la calidad de responsables de datos y **no requieren el consentimiento** del titular para efectuar el tratamiento de sus datos personales (art. 54).

#### **15. Disposiciones transitorias**

La ley establece diversas normas para asegurar una adecuada gradualidad en la implementación de la ley. Así, destacamos la entrada en vigencia *diferida* de la ley hasta el día primero del mes vigésimo cuarto posterior a la publicación de esta ley en el Diario Oficial. Es decir, hasta el **1° de diciembre de 2026** (artículo primero transitorio).

Por otra parte, es relevante considerar que los reglamentos de la ley deberán dictarse dentro de los 6 meses siguientes a su publicación. Es decir, a más tardar el 13 de junio de 2025 (artículo segundo transitorio).

También se establecen reglas especiales para la primera designación de los miembros del Consejo Directivo de la Agencia, la que, en todo caso, se realizará dentro de los 60 días *anteriores* a la entrada en vigencia de la presente ley (artículo cuarto transitorio).

## Comentario general

La ley en comento actualiza la normativa sobre protección de datos personales, para ponerla a la altura de los desafíos que representan las nuevas tecnologías y el creciente uso de datos que estas conllevan.

Respecto del modelo de protección, la ley se acerca bastante al **estándar europeo**, en particular al **Reglamento General de Protección de Datos (RGPD) de la Unión Europea** (Reglamento UE 2016/679, del 27 de abril de 2016). Este cuerpo normativo se caracteriza por requerir un consentimiento claro, específico, informado e inequívoco para el tratamiento de datos personales. Se trata, por lo demás, de un consentimiento esencialmente revocable, al igual que en la ley que comentamos. Asimismo, se les reconoce a los titulares el derecho a acceder, rectificar y suprimir sus datos personales, el derecho al olvido (es decir, a solicitar la supresión de datos personales bajo ciertas condiciones) y el derecho a la portabilidad de los datos. Al igual que en la nueva ley chilena, por lo demás, el tratamiento de datos sensibles está sujeto a restricciones más estrictas que el resto de los datos.

Respecto de las empresas y organizaciones responsables de datos, la norma europea establece diversas obligaciones, como aplicar medidas de seguridad adecuadas para proteger los datos personales, notificar las violaciones de seguridad de datos personales en un plazo máximo de 72 horas y, en algunos casos, definir un delegado de protección de datos. También se les exige el deber de proporcionar información clara sobre el tratamiento de datos personales y el cumplimiento de reglas de *accountability*.

Como hemos podido apreciar en este informe, casi todos estos elementos se encuentran contemplados en la nueva ley chilena. Así, se replica la norma del consentimiento informado, y se introducen diversos principios y deberes que los responsables de datos deberán aplicar, con su sistema correlativo de infracciones y sanciones para asegurar el cumplimiento de dichas normas. Por otro lado, se introducen nuevos derechos para los titulares de los datos, con sus respectivos procedimientos administrativos, también en línea con la legislación europea. Cabe mencionar, además, que ambas regulaciones establecen estándares para transferencias internacionales de datos, asegurando que se mantengan niveles adecuados de protección en los distintos ordenamientos jurídicos.

Ahora bien, respecto de la institucionalidad creada para fiscalizar y sancionar todas estas normas, se optó por la creación de una nueva entidad especializada. Aquí cabe mencionar que, una de las razones por las cuales se empujó este profundo cambio legislativo, fue la necesidad del país de contar con una autoridad de control de la protección de los datos personales. Ya desde antes del inicio de la tramitación de esta ley, existía un alto grado de consenso sobre esta necesidad, ya que la norma original de la ley N° 19.628 solamente regulaba el tratamiento de datos "y no un derecho

efectivo de los titulares a tener control sobre los mismos”<sup>2</sup>. Esto se debía, en gran parte, a la “inexistencia de un ente fiscalizador, de un procedimiento administrativo efectivo de reclamo y la falta de sanciones eficaces y disuasivas”<sup>3</sup>. Pero frente a esta necesidad, se vislumbraban dos modelos posibles: el primero implicaba concentrar este control en la misma entidad encargada del acceso a la información, como ocurre en México, en cuyo caso lo que correspondía era asignarle nuevas funciones y atribuciones al Consejo para la Transparencia; el segundo, en tanto, implicaba crear una agencia de protección de datos de carácter administrativo, independiente, especializado y con patrimonio propio, tal como ocurre en España.

La primera alternativa tenía como principal ventaja que permitía una adecuada resolución de los conflictos entre los diversos derechos en juego (en particular, entre el derecho a acceder a la información pública y el derecho a la privacidad y la protección de los datos personales)<sup>4</sup>. La segunda, en tanto, tenía como principal ventaja su especialización, además de que venía a llenar un vacío legal respecto de la regulación del sector privado, que hasta ese momento no contaba con una fiscalización similar al sector público<sup>5</sup>.

Finalmente, se optó por el modelo de la agencia independiente, en línea nuevamente con la legislación europea, particularmente española. Con todo, un remanente de este debate se puede apreciar en el artículo 31 de la ley, que establece el deber de coordinación regulatoria entre la Agencia de Protección de Datos Personales y el Consejo para la Transparencia.

Por último, cabe mencionar que la protección de los datos personales no se juega solamente en esta ley –aunque ella, ciertamente, establece los marcos generales de su protección–, sino también en otras normativas, como la **Ley Marco de Ciberseguridad** (ley N° 21.663), que al igual que la ley en comento es de promulgación reciente<sup>6</sup>. Dicha ley no crea solamente una nueva institucionalidad –particularmente, la Agencia Nacional de Ciberseguridad–, sino que además establece medidas para mejorar la respuesta de los órganos estatales frente a las amenazas cibernéticas, mejorando así también la seguridad de los datos personales.

Por otro lado, se discute actualmente un **proyecto de ley que regula la IA** (Boletín N° 16.821-19), ingresado el 7 de mayo de 2024. Se trata de un sistema modelado en

---

<sup>2</sup> ÁLVAREZ, Daniel. “Acceso a la información pública y protección de datos personales. ¿Puede el Consejo para la Transparencia ser la autoridad de control en materia de protección de datos?”, *Revista de Derecho de la Universidad Católica del Norte*, vol. 23, N° 1, Coquimbo, 2016, p. 62.

<sup>3</sup> *Ibíd.*, p. 63.

<sup>4</sup> Al respecto, sostiene Álvarez que “resulta una respuesta más consistente a la tensión entre ambas instituciones jurídicas, que sea un solo órgano el encargado de promover y proteger ambos derechos” (*Ibíd.*, p. 72).

<sup>5</sup> Véase: VERGARA ROJAS, Manuel. “Chile: Comentarios preliminares al proyecto de ley que regula la protección y tratamiento de datos personales y crea la Agencia de Protección de Datos Personales”, *Revista Chilena de Derecho y Tecnología*, vol. 6, N° 2, 2017, p. 141.

<sup>6</sup> Véase la minuta: SOTO, Víctor. “Descripción y síntesis de la ley N° 21.663, Ley Marco de Ciberseguridad”, Serie Minutas N° 48-24, Biblioteca del Congreso Nacional, 2024.

torno a la norma europea recientemente publicada (Reglamento (UE) 2024/1689). Así, además de inspirarse en la definición europea de "sistema de IA", el proyecto replica su enfoque general, basado en la definición de diversos niveles de riesgo y en la existencia de un verdadero sistema de gestión de riesgos, en los casos más graves. El punto es relevante por cuanto se prevé que el cumplimiento de estas normas sea fiscalizado, también, por Agencia de Protección de Datos Personales, creada por la ley que aquí comentamos.