90

COLECCIÓN
MATERIALES
DOCENTES

El nuevo sistema de protección de los datos personales

Carolina Riveros Ferrada
Eduardo Aldunate Lizana
Rommy Álvarez Escudero
Angela Arenas Massa

ACADEMIA JUDICIAL CHILE

2026

Carolina Riveros Ferrada

Doctora en Derecho, Ludwig-Maximilian-Universität; Múnich. Magíster en Derecho, (LL.M), Ruprecht-Karls-Universität Heidelberg. Licenciada en Ciencias Jurídicas, Pontificia Universidad Católica de Valparaíso, Chile. Abogada Corte Suprema de Chile. Profesora Titular de la Facultad de Ciencias Jurídicas y Sociales de la Universidad de Talca.

Eduardo Aldunate Lizana

Doctor en derecho por la Universidad del Sarre, Alemania. Licenciado en ciencias jurídicas. Facultad de Ciencias Jurídicas y Sociales, Universidad Católica de Valparaíso. Abogado, Corte Suprema de Chile. Profesor Titular de la Facultad de Derecho de la Pontificia Universidad Católica de Valparaíso, Chile.

Rommy Álvarez Escudero

Doctora en Derecho, Universidad Autónoma de Barcelona, Barcelona, España; Máster en Derecho de Familia, Universidad Autónoma de Barcelona, Barcelona, España; Magíster en Derecho, Pontificia Universidad Católica de Valparaíso, Valparaíso, Chile. Licenciada en Ciencias Jurídicas, Pontificia Universidad Católica de Valparaíso, Chile. Abogada Corte Suprema de Chile. Profesora Titular de la Facultad de Derecho Universidad de Valparaíso.

Angela Arenas Massa

Doctora en Historia y Teoría del Derecho Europeo, Universitá Tor Vergata; Roma. Magíster en Bioética y Formación, Universitá Catolica del Sacro Cuore, Roma. Licenciada en Ciencias Jurídicas y Sociales, Universidad Austral de Chile. Abogada Corte Suprema de Chile. Profesora Titular de la Facultad de Derecho de la Universidad Finis Terrae.

Los autores agradecen por el financiamiento del FONDECYT REGULAR de la Agencia Nacional de Investigación y Desarrollo, bajo el N°1230210 denominado "Protección a la privacidad, a la intimidad y a los datos personales (autodeterminación informativa) de los pacientes en el derecho chileno: revisión crítica a la luz de los estándares comparados e internacionales".

ACADEMIA JUDICIAL CHILE

El nuevos sistema de protección de los datos personales

MATERIALES DOCENTES 90

Amunátegui 465, Santiago de Chile

academiajudicial.cl • info@academiajudicial.cl

Resumen

El libro *El nuevo sistema de protección de datos personales* ofrece una exposición sistemática de un régimen moderno de tutela de datos personales, estructurado sobre principios, derechos y deberes exigibles. Para el juez, su aporte principal radica en clarificar el estatuto jurídico de garantías que se proyecta sobre el proceso, la prueba y la motivación de las decisiones. El texto desarrolla el contenido y alcance de los principios rectores (licitud, finalidad, proporcionalidad, minimización, seguridad, responsabilidad), enfatizando su función interpretativa y su valor como parámetros de control. Examina con precisión los derechos del titular y sus remedios, destacando la lógica de tutela efectiva y el estándar de diligencia del responsable. Asimismo, aborda la responsabilidad por infracción, incluyendo criterios de imputación, medidas correctivas y sanciones, con especial atención a la prevención de daños. Releva el rol de la autoridad de control y su interacción con los tribunales, particularmente en la delimitación de competencias y la revisión judicial. También estudia los desafíos probatorios en incidentes de seguridad y tratamientos automatizados, proponiendo estándares de evaluación razonables. En síntesis, el libro provee herramientas dogmáticas y prácticas para que la judicatura aplique el nuevo sistema como un derecho de protección reforzada, compatible con el debido proceso y con una comprensión actual de la vida digital.

Contenido

Abreviaturas

AAIP	Agencia de acceso a la información pública.
AEPD	Agencia española de protección de datos.
Agencia	Agencia de Protección de Datos Personales.
ANPD	*Autorida de Nacional de Proteção de Dados* / Autoridad nacional de protección de datos.
ARCO	Acceso, rectificación, cancelación y oposición.
BDSG	*Bundesdatenschutzgesetz* / Ley Federal de Protección de Datos.
BfDI	*Bundesbeauftragter für den Datenschutz und die Informationsfreiheit* / Encargado federal para la protección de datos y la libertad.
CADH	Convención Americana sobre Derechos Humanos
CCPA	*California Consumer Privacy Act* / Ley de privacidad del consumidor de California.
CDN	Convención sobre los derechos del niño.
CE	Comunidad Europea.
CEDH	Convenio Europeo para la protección de los derechos humanos y las libertades.
CETS	*Council of Europe Treaty Series. CTES 223: Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (2018).
CIDH	Corte Interamericana de Derechos Humanos.
CJI	Comité Jurídico Interamericano.
CNIL	*Commission Nationale de l'Informatique et des Libertés* / Comisión Nacional de Informática y Libertades.
COPPA	*Children's Online Privacy Protection Act* / Ley de protección de la privacidad en línea para niños.

CPR	Constitución Política de la República.
CPRA	*California Privacy Rights Act* / Ley de derechos de privacidad de California.
CS	Corte Suprema.
CSLI	*Cell-Site Location Information* (Información de ubicación derivada de las conexiones de un teléfono a antenas/torres celulares).
DPIA	*Data protection impact assessment* / Evaluación de impacto de protección de datos.
DUDH	Declaración Universal de Derechos Humanos.
EDPB	*European Data Protection Board* / Comité Europeo de Protección de Datos.
FRA	*European Union Agency for Fundamental Rights* / Agencia de los Derechos fundamentales de la Unión Europea.
GDPR	*General Data Protection Regulation* / Reglamento de Protección de Datos.
GG	*Grundgesetz* / Ley fundamental alemana.
HHS	*Health and Human Services* / Departamento de Salud y Servicios humanos.
HIPAA	*Health Insurance Portability and Accountability Act* / Ley de Portabilidad y Responsabilidad del Seguro Médico.
IA	Inteligencia artificial.
INAI	Instituto nacional de transparencia, acceso a la información y protección de datos personales.
LGPD	*Lei Geral de Proteção de Dados Pessoais* / Ley general de protección de datos.
LO	Ley Orgánica.
LOPD	Ley Orgánica de Protección de Datos.
LPDC	Ley de Protección de los Derechos de los Consumidores.
NNA	Niños, niñas y adolescentes.

OCDE	Organización para la Cooperación y el Desarrollo Económico.
OEA	Organización de los Estados Americanos.
OECD	Organización para la Cooperación y el Desarrollo Económico.
ONU	Organización de las Naciones Unidas.
RGPD	Reglamento General de Protección de Datos.
RIPD	Red Iberoamericana de Protección de Datos.
SEPD	Supervisor Europeo de Protección de Datos.
STC	Sentencia del Tribunal Constitucional español.
TC	Tribunal Constitucional.
TCE	Tribunal Constitucional españo.
TCF	Tribunal Constitucional Federal.
TEDH	Tribunal Europeo de Derechos Humanos.
TJUE	Tribunal de justicia de la Unión Europea.
UE	Unión Europea.
URCDP	Unidad reguladora y de control de datos personales.
UTM	Unidad Tributaria Mensual.
WP	*Working Party* / Equipo de trabajo

PRÓLOGO

La entrada en vigencia de la nueva normativa de protección de datos personales mediante la Ley 21.719 no constituye un simple perfeccionamiento técnico del régimen anterior, sino un cambio estructural en la manera en que el ordenamiento jurídico concibe la relación entre persona, información y poder. En una sociedad en que los datos personales se han convertido en infraestructura de la vida económica, administrativa y social, la protección de la vida privada deja de ser un asunto meramente defensivo para transformarse en una exigencia positiva del Estado constitucional y democrático de derecho. Este libro se inserta precisamente en ese punto de inflexión: propone una lectura sistemática de la nueva normativa desde la perspectiva de los derechos fundamentales, articulando la protección de datos personales como un presupuesto de autonomía individual, de igualdad material y de control jurídico frente a las asimetrías informacionales propias del entorno digital.

El primer mérito de la obra es situar la discusión en su dimensión histórica y comparada, reconstruyendo con precisión la evolución normativa sobre datos personales a nivel europeo, latinoamericano y nacional. Este enfoque permite comprender que el derecho de protección de datos no surge como una reacción episódica ante la innovación tecnológica, sino como resultado de una trayectoria doctrinal y jurisprudencial que ha ido reconociendo progresivamente la autodeterminación informativa como manifestación contemporánea de la dignidad humana. La comparación con el desarrollo europeo —en particular, con los modelos de autoridad de control, estándares de *accountability* y lógica de derechos— junto con el examen de experiencias latinoamericanas, ilumina tanto las convergencias como las tensiones que enfrenta Chile al adoptar un sistema más exigente en términos de cumplimiento, fiscalización y sanción. Lejos de ser una importación acrítica, el análisis comparado aquí desplegado opera como método de interpretación y como criterio de evaluación institucional.

Sobre esa base, el texto avanza hacia un marco conceptual y un estudio del ámbito de aplicación de la ley, abordando con rigor dogmático categorías que serán decisivas para la práctica: qué debe entenderse por dato personal, por tratamiento, por responsable y encargado, así como las hipótesis de exclusión,

las reglas de territorialidad y los desafíos derivados de tratamientos transfronterizos. En esta sección, el lector encontrará no solo definiciones, sino una propuesta de sistematización orientada a resolver problemas reales de calificación jurídica, especialmente relevantes en contextos de digitalización intensiva del sector público y privado. La claridad conceptual que el libro ofrece se vuelve indispensable para evitar que la aplicación del nuevo régimen derive en formalismos vacíos o en interpretaciones contradictorias que debiliten su función garantista.

En el núcleo de la obra se examinan los principios informadores y las bases de legitimidad del tratamiento, así como la posición jurídica de los titulares, sus derechos y las obligaciones correlativas de quienes tratan datos. El texto demuestra que el sistema no puede reducirse al consentimiento entendido como acto aislado, sino que exige una comprensión compleja de la licitud, la proporcionalidad y la finalidad, especialmente frente a fenómenos como la toma de decisiones automatizadas, la reutilización masiva de datos y la tensión entre innovación y garantías. Al abordar los derechos del titular —acceso, rectificación, supresión, oposición, portabilidad y otros— junto con los deberes de seguridad, transparencia y responsabilidad proactiva, el libro se sitúa en el corazón del nuevo paradigma: el tránsito desde una lógica de mera declaración normativa hacia una lógica de cumplimiento verificable, donde la protección de datos se convierte en gobernanza jurídica de la información personal.

La obra culmina con un aporte especialmente valioso para la dogmática y la práctica forense: el estudio de las acciones judiciales vinculadas a datos personales y la responsabilidad civil derivada de la infracción al derecho de protección de datos. Este desarrollo resulta crucial, porque la eficacia de la ley no dependerá solo de su arquitectura institucional o de la amenaza sancionatoria, sino también de la posibilidad real de obtener tutela judicial efectiva y reparación frente al daño. En un escenario donde la vulneración de datos puede afectar simultáneamente la honra, la privacidad, la identidad y la esfera patrimonial de las personas, la responsabilidad civil se presenta como un mecanismo de justicia correctiva que debe dialogar con el régimen administrativo sin diluirse en él. Este libro ofrece, en consecuencia, una contribución a diferentes operadores de la disciplina del Derecho: no solo explica la Ley 21.719, sino que propone claves interpretativas para su aplicación coherente, asegurando que la protección de datos en Chile se consolide como un verdadero derecho garantizado y no como una promesa normativa de cumplimiento incierto.

Es preciso indicar que este libro es parte de la investigación financiada por FONDECYT REGULAR de la Agencia Nacional de Investigación y Desarrollo, bajo el N°1230210 denominado "Protección a la privacidad, a la intimidad y a los datos personales (autodeterminación informativa) de los pacientes en el derecho chileno: revisión crítica a la luz de los estándares comparados e internacionales". Huelgan también nuestros agradecimientos a Paulina Arratia Rojas, personal técnico del proyecto, quien contribuyó con la revisión de los aspectos formales del texto. Finalmente, agradecemos a la Academia Judicial de Chile por propiciar el análisis y revisión de una materia actual en que Chile adopta estándares internacionales que imponen relevantes desafíos a los operadores jurídicos.

Los autores

Valparaíso y Santiago, verano de 2026

Introducción

La presente monografía surge como respuesta a la necesidad de contar con un texto de consulta completo y comprensivo sobre el nuevo sistema de protección de datos personales en Chile, particularmente tras las transformaciones radicales introducidas por la Ley 21.719 (D.O.13.12.2024, con vigencia diferida para el 01.12.2026) a la Ley 19.628 sobre Protección a la vida privada. Su propósito fundamental es proveer a la comunidad jurídica de una herramienta de manejo sencillo que permita el conocimiento tanto de los principales aspectos teóricos como de la proyección práctica de las materias tratadas, facilitando la transición desde el marco regulatorio previo hacia el nuevo paradigma de protección de datos que se alinea con los estándares internacionales más exigentes. Este trabajo aspira a convertirse en un referente tanto para la interpretación dogmática de las nuevas normas como para su aplicación práctica en los diversos contextos en que opera el derecho de protección de datos personales.

Este libro va dirigido a lectores con conocimientos previos de diversas disciplinas del derecho. Se presenta un análisis sistemático del nuevo sistema chileno de protección de datos, situándolo en el contexto comparado, internacional y regional. Este enfoque permite comprender no solo las particularidades del desarrollo nacional, sino también las influencias que han moldeado la reciente evolución del derecho chileno. La perspectiva comparada resulta esencial para anticipar desarrollos futuros y para facilitar la interpretación de normas que han sido inspiradas en experiencias extranjeras.

De particular relevancia se considera en el contexto chileno contemporáneo la contribución al desarrollo de una cultura de protección de datos que vaya más allá del cumplimiento normativo. Se trata de un punto de partida para una comprensión profunda de los valores y principios que subyacen al derecho de protección de datos, entendido como manifestación del derecho fundamental a la autodeterminación informativa y, en última instancia, de la dignidad humana en la era digital.

El texto aspira también a facilitar el diálogo entre diferentes actores del sistema: jueces, abogados litigantes, académicos, y eventualmente, los operadores de la nueva Agencia de Protección de Datos Personales.

I. Estructura y contenidos

La estructura de esta monografía ha sido diseñada para ofrecer una progresión lógica desde los fundamentos conceptuales hacia las aplicaciones prácticas más específicas.

El primer componente sustantivo aborda la evolución normativa sobre datos personales a nivel europeo, latinoamericano y nacional. Este capítulo establece el contexto histórico y comparado necesario para comprender el desarrollo del derecho chileno de protección de datos. Se analiza detalladamente la influencia del modelo europeo, desde el Convenio 108 del Consejo de Europa hasta el Reglamento General de protección de datos -en adelante RGPD-, así como la evolución específica del modelo latinoamericano, desde las primeras incorporaciones constitucionales del *Hábeas data* hasta las legislaciones contemporáneas más sofisticadas. Esta perspectiva comparada permite situar la experiencia chilena en su contexto regional e internacional.

El marco conceptual y ámbito de aplicación de la ley de datos personales constituye el segundo elemento estructural de la monografía. Este capítulo desarrolla las definiciones fundamentales establecidas en la Ley 21.719, particularmente el concepto amplio de datos personales que adopta la legislación chilena. Se analiza el ámbito de aplicación material y territorial de la ley, incluyendo sus efectos extraterritoriales, y se establecen las distinciones conceptuales necesarias para la correcta aplicación de la normativa. Especial atención se dedica a las categorías especiales de datos personales y a los regímenes específicos que la ley establece para diferentes tipos de tratamiento.

Los principios informadores y bases de legitimidad del tratamiento de datos personales constituyen el núcleo dogmático del sistema. Este capítulo analiza exhaustivamente los siete principios fundamentales que orientan todo tratamiento legítimo: licitud, lealtad y transparencia; limitación de la finalidad; minimización de datos; exactitud; limitación del plazo de conservación; integridad y confidencialidad; y responsabilidad proactiva (*accountability*). Cada principio es examinado tanto en su dimensión conceptual como en sus implicancias prácticas, estableciendo criterios interpretativos y estándares de aplicación. Paralelamente, se desarrollan las bases de legitimidad del tratamiento, analizando cuándo el consentimiento es necesario y cuándo pueden aplicarse otras bases legales.

El tratamiento de titulares y grupos vulnerables merece atención especial, reconociendo que la protección de datos debe adaptarse a las circunstancias específicas de diferentes categorías de personas. Se analiza detalladamente el régimen de protección reforzada que la ley establece para niños, niñas y adolescentes -en lo sucesivo NNA-, incluyendo las complejas cuestiones relacionadas con el consentimiento y la capacidad jurídica en el entorno digital. También se examinan las protecciones específicas para otros grupos que pueden requerir consideraciones especiales, como personas con discapacidad o personas mayores.

Los derechos y obligaciones asociados al tratamiento de datos personales es una parte importante del texto. En cuanto a derechos, se desarrollan exhaustivamente no solo los derechos ARCO tradicionales (acceso, rectificación, cancelación y oposición), sino también los nuevos derechos introducidos por la legislación moderna: portabilidad de datos, limitación del tratamiento, y oposición a decisiones individuales automatizadas. Cada derecho es analizado en cuanto a sus presupuestos, alcance, procedimientos de ejercicio y límites. En el ámbito de las obligaciones, se examinan detalladamente los deberes que la ley impone a responsables y encargados del tratamiento, incluyendo las obligaciones de información y transparencia, adopción de medidas de seguridad, protección desde el diseño y por defecto, y reporte de vulneraciones.

Las acciones judiciales vinculadas a datos personales abordan los mecanismos de tutela disponibles para la protección efectiva de los derechos. Se analiza tanto la tutela administrativa ante la nueva Agencia de Protección de Datos Personales -en adelante, Agencia-, como los remedios jurisdiccionales tradicionales, incluyendo el recurso de protección constitucional y las acciones civiles. Especial atención se dedica a la articulación entre estas diferentes vías de tutela y a los criterios para determinar cuándo es apropiado recurrir a cada una de ellas.

La responsabilidad civil por infracción al derecho de datos personales completa el análisis de los mecanismos de protección, examinando tanto el régimen de responsabilidad establecido específicamente en la Ley 21.719 como la aplicación de las reglas generales de responsabilidad civil. Se analizan los presupuestos de la responsabilidad, los criterios de imputación, y los tipos de daños resarcibles, incluyendo el complejo tema del daño extrapatrimonial en contextos de violación de la privacidad.

Conforme a los lineamientos de la Academia Judicial para este tipo de textos, se incorporan herramientas específicamente diseñadas para responder a las necesidades inmediatas de los operadores jurídicos en su uso cotidiano.

El glosario proporciona definiciones precisas y accesibles de los términos técnicos utilizados tanto en la Ley 21.719 como en la doctrina y jurisprudencia especializada nacional e internacional, facilitando la comprensión de conceptos que a menudo presentan complejidades semánticas o provienen de tradiciones jurídicas diversas. La sección de preguntas y respuestas, por su parte, aborda situaciones concretas que pueden enfrentar académicos, abogados y jueces en su desempeño profesional.

Desafíos contemporáneos y relevancia práctica

El derecho de protección de datos personales enfrenta en el presente desafíos inéditos que trascienden los marcos normativos tradicionales donde el advenimiento de la inteligencia artificial y las decisiones automatizadas representan quizás el desafío más complejo para el derecho de protección de datos contemporáneo. Estas tecnologías amplifican las capacidades de predicción, perfilamiento y decisión, incrementando exponencialmente los riesgos de discriminación algorítmica, vigilancia masiva y opacidad en la toma de decisiones públicas y privadas. La Ley 21.719 incorpora protecciones específicas contra decisiones exclusivamente automatizadas, estableciendo el derecho a no ser objeto de tales decisiones cuando produzcan efectos jurídicos o afecten significativamente al titular. Se aportan los criterios para determinar cuándo una decisión debe considerarse "exclusivamente automatizada" y qué constituye "afectación significativa".

El procesamiento masivo de datos personales (*Big Data*) y el perfilamiento algorítmico plantean desafíos particulares para principios tradicionales como la minimización de datos y la limitación de finalidad. El texto examina cómo estos principios deben reinterpretarse en contextos donde el valor de los datos a menudo emerge de su procesamiento conjunto y donde las finalidades pueden evolucionar dinámicamente. Se analizan las tensiones entre la innovación tecnológica y la protección de derechos fundamentales, y se proponen criterios para lograr equilibrios adecuados.

La transferencia internacional de datos constituye otro ámbito de particular complejidad práctica y relevancia estratégica en una economía globalizada. La Ley 21.719 incorpora un modelo directamente inspirado en el RGPD, adoptando el principio de adecuación sustancial del nivel de protección, conforme al cual los datos personales solo pueden transferirse a terceros países o destinatarios internacionales que aseguren garantías equivalentes a las previstas por el ordenamiento jurídico chileno. Este modelo busca preservar la unidad del estándar de tutela y evitar que la salida transfronteriza

de datos se convierta en una forma de eludir las obligaciones impuestas dentro del territorio nacional. El texto desarrolla los criterios para evaluar la adecuación del nivel de protección extranjero, considerando no solo la existencia de normas formales, sino también la efectividad de su aplicación, la independencia de las autoridades de control, y la disponibilidad de recursos judiciales efectivos. Se examinan detalladamente los instrumentos disponibles para legitimar transferencias, incluyendo cláusulas contractuales tipo que establezcan obligaciones específicas para el receptor de los datos, normas corporativas vinculantes para grupos empresariales multinacionales, y las excepciones que la ley permite en circunstancias especiales. Esta materia resulta de particular importancia para empresas que operan internacionalmente, y para Chile en su aspiración de obtener lo que se conoce como una "decisión de adecuación" por parte de la Unión Europea, lo que facilitaría significativamente los flujos de datos con ese espacio económico.

La creación de la Agencia como autoridad administrativa independiente representa una innovación institucional fundamental en el sistema jurídico chileno, que transita desde un modelo de tutela exclusivamente jurisdiccional hacia un sistema dual que combina supervisión administrativa especializada y control judicial. La tutela administrativa establece un sistema de supervisión ex ante que complementa los remedios judiciales tradicionales. El texto analiza las competencias y procedimientos de la Agencia, así como su articulación con otras autoridades administrativas y con el Poder Judicial.

El principio de *accountability* y las evaluaciones de impacto representan un cambio paradigmático desde un modelo reactivo hacia uno preventivo de protección de datos. Este enfoque exige que los responsables del tratamiento no solo cumplan con la ley, sino que puedan demostrar su cumplimiento mediante medidas técnicas y organizativas adecuadas. Se examinan los criterios para la instalación efectiva de la *accountability*, incluyendo la realización de evaluaciones de impacto en protección de datos y el establecimiento de sistemas de gestión de riesgos.

La convergencia con estándares internacionales, particularmente el RGPD y las Directrices de la OCDE, sitúa al derecho chileno en un contexto global de armonización normativa. Esta convergencia no es meramente técnica, sino que responde a la aspiración de Chile de obtener una decisión de adecuación por parte de la Unión Europea, lo que facilitaría significativamente los flujos de datos transfronterizos y fortalecería la inserción del país en la economía digital global.

El rol del juez en la era digital experimenta transformaciones significativas que requieren nuevas competencias, enfoques metodológicos y herramientas

conceptuales. En el nuevo sistema de protección de datos, los jueces deben ahora evaluar no solo la existencia de daños o infracciones específicas, sino también la suficiencia y adecuación de las medidas de diligencia, seguridad y gestión de riesgos adoptadas por los responsables del tratamiento conforme al principio de *accountability*. Esta labor exige familiaridad con conceptos técnicos complejos propios de la informática y las ciencias de datos, comprensión de los modelos de negocio digitales, y capacidad para equilibrar innovación tecnológica con protección efectiva de derechos fundamentales. El juez debe aplicar tests de proporcionalidad sofisticados que consideren no solo la afectación individual, sino también los efectos sistémicos del tratamiento de datos a gran escala. Además, la función judicial se ve enriquecida por la interacción con la Agencia, cuyas resoluciones, directrices e interpretaciones técnicas constituyen referentes interpretativos relevantes, aunque no vinculantes, para el control jurisdiccional.

El desafío fundamental reside en lograr un equilibrio adecuado entre innovación tecnológica y protección de derechos fundamentales, considerando que es un tema en constante evolución. Este equilibrio no puede lograrse mediante fórmulas abstractas, sino que requiere análisis casuístico sofisticado que incluya múltiples factores: la naturaleza de los datos tratados, las finalidades del tratamiento, los riesgos para los titulares, los beneficios sociales de la innovación, y la disponibilidad de medidas de mitigación.

En síntesis, los datos personales no son meramente activos económicos o insumos tecnológicos, sino manifestaciones de la personalidad e identidad individual que merecen protección en cuanto tales. Esta perspectiva humanista debe permear toda interpretación y aplicación del derecho de protección de datos, asegurando que el progreso tecnológico se desarrolle al servicio de la persona humana y no a expensas de su autonomía y dignidad.

Los desafíos que enfrenta Chile en la implementación efectiva del nuevo sistema de protección de datos son múltiples y significativos. Será necesario desarrollar capacidades institucionales en la Agencia, formar especialistas en la judicatura y la abogacía, sensibilizar a las empresas y organizaciones sobre sus nuevas obligaciones, y educar a la ciudadanía sobre sus derechos.

Capitulo 1
Vida privada y protección de datos

I. El derecho a la privacidad y su desarrollo constitucional

El derecho a la privacidad constituye uno de los desarrollos más significativos (y al mismo tiempo complejos) del constitucionalismo contemporáneo, emergiendo como respuesta a las transformaciones sociales, tecnológicas y políticas producidas desde finales del siglo XIX. Desde la formulación de Warren y Brandeis[1] del "*right to be let alone*" (derecho a ser dejado en paz) hasta los actuales desafíos de la inteligencia artificial y el denominado "capitalismo de vigilancia", la privacidad ha evolucionado desde una conceptualización del derecho de daños en el derecho privado del *common law* hacia un derecho fundamental complejo y multidimensional que permea múltiples áreas del ordenamiento jurídico[2].

Esta evolución no ha sido uniforme ni lineal. Los sistemas constitucionales han desarrollado aproximaciones diversas al derecho a la privacidad, reflejando diferencias en tradiciones jurídicas, experiencias históricas, estructuras institucionales y valores culturales. Mientras en Estados Unidos la concepción de la privacidad se ha desarrollado como privacidad decisional vinculada al debido proceso sustantivo, Alemania ha desarrollado la noción de autodeterminación informacional desde la dignidad humana, España ha establecido un sistema de protección en el artículo 18 de su Constitución, y Chile mantiene una formulación más tradicional centrada en vida privada y honra[3].

En el siglo XXI, los avances tecnológicos plantean nuevos desafíos. La dimensión del denominado "*Big Data*", la inteligencia artificial, las insospechadas proyecciones del "Internet de las Cosas", y los modelos de negocio basados en la extracción de datos personales han generado lo que Shoshana Zuboff[4] denomina "capitalismo de vigilancia", desafiando los marcos normativos tradicionales y exigiendo nuevas respuestas constitucionales. En este

[1] Warren y Brandeis (1890).

[2] Zuboff (2019: 10).

[3] Whitman (2004: 1151).

[4] Zuboff (2019:10).

contexto, una mirada comparada aporta a una comprensión integral del problema destinada a facilitar al lector la elaboración de criterios y argumentos al momento de enfrentar problemas que puedan afectar al ámbito protegido por el artículo 19 N°4 de la Constitución chilena. El marco temporal permite capturar la evolución completa del derecho a la privacidad, desde sus orígenes doctrinales hasta los desafíos contemporáneos. Aparte de Chile, la selección de Estados Unidos, Alemania, y España persigue levantar una muestra representativa de diferentes tradiciones jurídicas (*common law* vs. derecho continental), experiencias históricas diversas (democracias consolidadas vs. transiciones democráticas), y niveles variados de desarrollo normativo en protección de datos. Esta selección permite examinar tanto las particularidades nacionales como los procesos transnacionales de difusión normativa, con énfasis en la evolución jurisprudencial. En todo caso, esta selección, aunque representativa, no agota la diversidad de aproximaciones constitucionales a la privacidad a nivel global. En este capítulo se abordará exclusivamente la dimensión constitucional del derecho a la privacidad, excluyendo desarrollos en áreas como derecho civil, penal o administrativo, salvo cuando sean directamente relevantes para la interpretación constitucional.

II. Conceptos

A fin de lograr un sustrato común para el estudio del derecho a la privacidad en distintas jurisdicciones, es menester realizar algunas precisiones. Sin perjuicio de que el ámbito protegido por el derecho a la privacidad admite un adecuado tratamiento dogmático en la distinción entre derecho a la privacidad como no exposición (derecho a la no "publificación" de información sobre una persona cuando dicha información carece de interés o relevancia pública); como protección a la intimidad (derecho a la no intromisión en un ámbito que por su naturaleza o contexto no debe ser conocido por terceros salvo decisión del titular del derecho) y como protección de datos, el análisis comparado hace aconsejable el uso de las categorías más generales que se han ido consolidando en la doctrina y jurisprudencia de otros países. Para estos efectos, adoptamos entonces las siguientes definiciones operativas que permiten distinguir entre las diferentes dimensiones de la privacidad y precisar su relación con conceptos afines como la protección a la honra (o el honor, según la fuente que se tenga a la vista) y la protección de datos personales.

1. Privacidad decisional

La privacidad decisional, también denominada privacidad autónoma o sustantiva, se refiere al derecho fundamental que protege la capacidad del individuo para tomar decisiones autónomas sobre aspectos íntimos de su existencia, particularmente en materia de reproducción, sexualidad, matrimonio, planificación familiar y relaciones afectivas, sin interferencia gubernamental injustificada[5]. Esta dimensión de la privacidad encuentra su máxima expresión en la jurisprudencia constitucional estadounidense, donde ha sido desarrollada a partir de la cláusula del debido proceso sustantivo de la Decimocuarta Enmienda.

Las características distintivas de la privacidad decisional incluyen: (a) autodeterminación reproductiva, que abarca decisiones sobre contracepción, procreación y, como objeto de controversia sostenida, la interrupción del embarazo; (b) libertad de elección en relaciones íntimas, incluyendo orientación sexual e identidad de género; (c) protección contra interferencia gubernamental en decisiones personales fundamentales; y (d) dimensión sustantiva del debido proceso que trasciende garantías meramente procedimentales. Esta conceptualización ha sido fundamental en casos como *Griswold v. Connecticut* (1965), *Eisenstadt v. Baird* (1972), *Roe v. Wade* (1973), y *Lawrence v. Texas* (2003), aunque ha enfrentado retrocesos significativos con *Dobbs v. Jackson* (2022).

2. Privacidad especial y comunicacional

La privacidad espacial y comunicacional comprende la protección de la intimidad del domicilio, correspondencia y comunicaciones contra intrusiones no autorizadas por parte del Estado o terceros[6]. Esta dimensión tiene raíces históricas profundas en el *common law* inglés, particularmente en el principio "*a man's house is his castle*", y se encuentra codificada en la Cuarta Enmienda estadounidense, el artículo 10 de la *Grundgesetz* alemana, y los artículos 18.2 y 18.3 de la Constitución española.

Sus elementos constitutivos incluyen: (a) inviolabilidad del domicilio, entendido no solo como residencia física sino como espacio de intimidad familiar; (b) secreto de las comunicaciones, que abarca correspondencia postal, telefónica, electrónica y digital; (c) protección contra registros e

[5] Rubenfeld (1989:737).

[6] Kerr (2004:801).

incautaciones no razonables, sujeto a requisitos de orden judicial previa salvo circunstancias excepcionales; y (d) expectativa razonable de privacidad como criterio determinante de la protección constitucional. La evolución tecnológica ha expandido significativamente el alcance de esta protección, incorporando comunicaciones digitales, datos de ubicación, y contenidos almacenados en dispositivos electrónicos. Si bien desde el punto de vista de un tratamiento riguroso del ámbito protegido de cada uno de los derechos involucrados (secreto de las comunicaciones, inviolabilidad del hogar, etc.) esta figura merece críticas sustantivas.

3. Privacidad informacional

La privacidad informacional, conceptualizada por primera vez por el Tribunal Constitucional Federal alemán como "*Recht auf informationelle Selbstbestimmung*" (derecho a la autodeterminación informacional) en la sentencia del censo de 1983, se refiere al derecho del individuo a controlar cuándo, y bajo qué límites, los datos relativos a su vida privada pueden ser comunicados a otros.[7] Esta dimensión ha adquirido relevancia central en la era digital, constituyendo el fundamento conceptual de la moderna protección de datos personales.

Los componentes esenciales de la privacidad informacional comprenden: (a) control sobre datos personales, incluyendo decisiones sobre su recolección y tratamiento; (b) consentimiento informado como base legitimadora del procesamiento; (c) principios de proporcionalidad y finalidad en el uso de información personal; (d) derechos de acceso, rectificación, cancelación y oposición (derechos ARCO); y (e) derecho al olvido y portabilidad de datos en contextos digitales. Esta conceptualización ha influido decisivamente en el desarrollo del derecho europeo de protección de datos, desde la Directiva 95/46/CE hasta el actual RGPD.

4. Distinción entre privacidad y honor (España) u honra (Chile)

La distinción entre privacidad y honor ha generado confusión doctrinal y jurisprudencial, particularmente en sistemas del derecho continental, donde ambos derechos coexisten en los textos constitucionales. Mientras

[7] Rouvroy y Poullet (2009: 45), en especial, sobre la base del derecho de autodeterminación de la persona.

la privacidad protege información y decisiones personales independientemente de su veracidad o impacto en la reputación social, el honor u honra protegen específicamente la reputación social contra afirmaciones falsas, inexactas o injuriosas. La privacidad es esencialmente defensiva —busca excluir intromisiones en la esfera personal—mientras el honor es reactivo: responde a ataques a la reputación. Ambos derechos pueden verse afectados simultáneamente por divulgaciones no autorizadas, pero responden a bienes jurídicos distintos: autodeterminación personal versus reputación social.

5. Privacidad versus protección de datos personales

La relación entre privacidad y protección de datos personales es compleja y ha evolucionado significativamente en las últimas décadas. Mientras la privacidad constituye un derecho fundamental amplio que incluye autodeterminación informacional, la protección de datos personales representa un marco de condiciones bajo las cuales el procesamiento de datos es legítimo[8]. La protección de datos opera como manifestación específica del derecho más amplio a la privacidad, estableciendo principios operativos (licitud, lealtad, transparencia, limitación de finalidad, minimización, exactitud, limitación de plazo, integridad y confidencialidad) y derechos específicos (información, acceso, rectificación, supresión, limitación del tratamiento, portabilidad, oposición). Sin embargo, la protección de datos también trasciende la privacidad individual, incorporando objetivos de regulación del mercado digital y protección de la competencia.

Este marco conceptual permite un análisis más preciso de las diferentes dimensiones del derecho constitucional a la privacidad y sus desarrollos específicos en cada jurisdicción. Esta taxonomía reconoce que la privacidad no constituye un derecho monolítico sino un conjunto de protecciones interrelacionadas que responden a diferentes amenazas y valores constitucionales. La comprensión de estas distinciones es esencial para evaluar comparativamente los desarrollos jurisprudenciales y normativos en Estados Unidos, Alemania, España y Chile, identificando convergencias y divergencias en la protección de cada dimensión específica de la privacidad.

[8] De Hert y Gutwirth (2009).

III. Estados Unidos: Evolución de la Privacidad Decisional y Espacial

1. Contexto histórico y constitucional

El desarrollo del derecho a la privacidad en Estados Unidos presenta características únicas derivadas de la ausencia de su reconocimiento constitucional expreso. La Constitución de 1787 y la *Bill of Rights* de 1791 no mencionan explícitamente la "privacidad". Sin embargo, la Cuarta Enmienda (1791) establece protección contra "registros e incautaciones no razonables", mientras la Decimocuarta Enmienda (1868) introduce, dentro de los derechos que operan a nivel estadual, la cláusula del debido proceso, que se convertirá en fundamento de la privacidad decisional. Este "anclaje constitucional" ha permitido desarrollo jurisprudencial creativo, pero también controversias persistentes sobre legitimidad y límites del derecho.

2. Evolución Jurisprudencial

2.1. Era Fundacional (1886-1928)

La conceptualización moderna de la privacidad estadounidense emerge en la era industrial tardía. Boyd v. United States[9] estableció conexiones entre Cuarta y Quinta enmiendas, reconociendo la protección constitucional de documentos privados contra requisiciones gubernamentales. La Corte declaró que compeler producción de documentos privados equivalía a autoincriminación forzada, estableciendo precedente para protección informacional primitiva. Más significativo fue el artículo de Warren y Brandeis[10], "*The Right to Privacy*", que señaló que existe un derecho a ser dejado en paz "*right to be let alone*" con base en el derecho común (no en el derecho constitucional) como protección frente a daños (*tort*) contra intrusiones mediáticas. Aunque académico, este artículo influyó profundamente en desarrollos jurisprudenciales posteriores. Olmstead v. United States[11] representó retroceso inicial, con la mayoría de la Corte negando protección constitucional a escuchas telefónicas sin entrada física. Sin embargo, la disidencia visionaria del Juez Brandeis anticipó desafíos tecnológicos futuros, declarando que "*the right to be let alone*" constituía "*the most comprehensive of rights and the right most valued by civilized men*".

[9] Boyd v. United States, sentencia de fecha 1de febrero de 1886.

[10] Warren y Brandeis (1890).

[11] Olmstead v. United States, sentencia de fecha 4 de junio de 1928.

2.2. Era de reconocimiento constitucional (1965-1980)

Griswold v. Connecticut[12] marca el nacimiento de la privacidad en el moderno derecho constitucional de los Estados Unidos. La Corte Suprema, bajo presidencia de Earl Warren, invalidó una ley que prohibía anticonceptivos, reconociendo el derecho implícito a la privacidad matrimonial. El juez Douglas desarrolló la teoría de las "penumbras" y "emanaciones" de la *Bill of Rights*, argumentando que derechos específicos, en su intersección, crean zonas de privacidad. Este método interpretativo, aunque controversial, estableció precedente para el reconocimiento de derechos fundamentales implícitos. Katz v. United States[13] revolucionó el núcleo de lo que aquí hemos llamado privacidad espacial, reemplazando el test de "*trespass*" (proveniente de la argumentación en *The Right of Privacy*) por la "expectativa razonable de privacidad". La formulación del juez Harlan —expectativa subjetiva de privacidad que la sociedad reconoce como razonable— se convirtió en estándar dominante para casos de Cuarta Enmienda. Eisenstadt v. Baird[14] individualiza el derecho de privacidad, extendiendo la protección anticonceptiva a personas solteras y estableciendo que la privacidad protege decisiones individuales, no solo relaciones matrimoniales.

2.3. Leading cases contemporáneos

Roe v. Wade[15] representa la máxima expresión —y la de mayor controversia— de la privacidad decisional estadounidense. La Corte reconoció límites a la competencia estatal para prohibir el aborto bajo el concepto de privacidad reproductiva, estableciendo un marco que buscaba conciliar o balancear los derechos maternos con los intereses estatales. La decisión generó oposición política sostenida y fragmentación jurisprudencial que culminó con su reversión en Dobbs v. Jackson[16]. Lawrence v. Texas[17] revitalizó privacidad decisional *post-Bowers*, invalidando leyes que castigaban la sodomía y reconociendo autonomía sexual bajo *liberty clause*. Esta decisión preparó el fundamento para Obergefell v. Hodges[18] sobre matrimonio

[12] Griswold v. Connecticut, sentencia de fecha 7 de junio de 1965.

[13] Katz v. United States, sentencia de fecha 18 de diciembre de 1967.

[14] Eisenstadt v. Baird, sentencia de fecha 22 de marzo de 1972.

[15] Roe v. Wade, sentencia de fecha 22 de enero de 1973.

[16] Dobbs v. Jackson, sentencia de fecha 24 de junio de 2022.

[17] Lawrence v. Texas, sentencia de fecha 26 de junio de 2003.

[18] Obergefell v. Hodges, sentencia de fecha 26 de junio de 2015.

igualitario. En privacidad espacial, Riley v. California[19] aplicó protecciones constitucionales a era digital, requiriendo una orden judicial para el registro de teléfonos celulares. La Corte reconoció que estos dispositivos contienen la "suma de la vida privada de un individuo", estableciendo una protección robusta para dispositivos digitales. Carpenter v. United States[20] extendió la protección a datos de ubicación CSLI, adaptando el estándar de "expectativa razonable de privacidad" *para Big Data* y vigilancia digital masiva.

3. Marco legislativo sectorial

Estados Unidos adoptó un enfoque sectorial para protección de datos, en contraste con los modelos europeos de aproximación comprehensiva. La *Privacy Act* de 1974 regula el tratamiento de información personal por agencias federales, estableciendo principios de propósito limitado, acceso individual y corrección de datos. La *Health Insurance Portability and Accountability Act* (HIPAA (1996)) protege información médica con estándares estrictos para "*covered entities*". La *Children's Online Privacy Protection Act* (COPPA (1998)) regula la recolección de datos en línea de menores de edad, requiriendo consentimiento parental. A nivel estadual, la *California Consumer Privacy Act* CCPA (2018) y su sucesora la CPRA (2020) establecieron derechos similares a los de estándar europeo: conocer, eliminar, *opt-out* y no discriminación.

4. Debates doctrinales y tensiones contemporáneas

En Estados Unidos el derecho a la privacidad enfrenta múltiples controversias en la actualidad. Dobbs v. Jackson[21] eliminó la protección constitucional federal del aborto, fragmentando el paisaje legal y cuestionando la permanencia de la concepción de privacidad decisional que se había mantenido durante cuarenta años. Algunos estados han prohibido el aborto, mientras que otros fortalecen la protección a este derecho, creando un verdadero mosaico legal. Por su parte, la inteligencia artificial, el reconocimiento facial y el denominado "capitalismo de vigilancia" desafían los marcos normativos del siglo pasado. La doctrina del "tercero" (*Third-party doctrine*) ha permitido el acceso gubernamental a datos en manos de empresas privadas, limitando la protección de la privacidad de quienes trabajan en ellas. De este modo, el debate constitucional sobre la privacidad en Estados Unidos se encuentra activo y lejos de asentarse.

[19] Riley v. California, sentencia de fecha 25 de junio de 2014.

[20] Carpenter v. United States, sentencia de fecha 22 de junio de 2018.

[21] Dobbs v. Jackson, sentencia de fecha 24 de junio de 2022.

IV. Alemania: Autodeterminación informacional y dignidad humana

1. Contexto histórico y constitucional

El desarrollo alemán del derecho a la privacidad está intrínsecamente vinculado a la experiencia histórica del régimen nazi y la fundación de la República Federal en 1949. La *Grundgesetz* (Ley Fundamental) estableció la dignidad humana como principio supremo (artículo 1.1) y el libre desarrollo de la personalidad (artículo 2.1) como derechos fundamentales, creando una base constitucional sólida para la protección de la privacidad. La experiencia totalitaria generó particular sensibilidad hacia la recolección estatal de información personal, influyendo decisivamente en la jurisprudencia del *Bundesverfassungsgericht* (Tribunal Constitucional Federal, TCF). Esta base permitió desarrollos jurisprudenciales que, particularmente en protección de datos personales, han influido globalmente en el constitucionalismo de la privacidad[22].

2. Desarrollo del derecho general de personalidad

El TCF desarrolló creativamente el "*allgemeines Persönlichkeitsrecht*" (derecho general de personalidad) combinando la protección a la dignidad humana (artículo 1.1) y el libre desarrollo de la personalidad (artículo 2.1). La sentencia del TCF en el caso Elfes (1957) estableció una interpretación amplia del artículo 2.1 como "*allgemeine Handlungsfreiheit*" (libertad general de acción), sentando bases para expansión de derechos fundamentales. Los casos de personalidad de los años 1950-1960 consolidaron este derecho implícito, protegiendo la esfera íntima, el honor, la imagen y la autodeterminación personal. La sentencia TCF en el caso Lebach (1973) refinó la metodología de ponderación (*Abwägung*) entre personalidad y libertad de expresión, estableciendo criterios de balance entre el interés actual de la información versus la protección de la personalidad. Esta jurisprudencia creó un marco conceptual que permitiría desarrollos posteriores en protección de datos y derechos digitales.

[22] Whitman (2004:1151); El Tribunal Constitucional Federal construyó parte importante de su jurisprudencia en base a la obra "Comentario a la Ley Fundamental" de Theodor Maunz y Günther Dürig, publicado en formato de archivo con hojas reemplazables desde 1958. Desde 2021 el comentario recibe la denominación *Dürig/Herzog/Scholz.*

3. La Revolución de la autodeterminación informacional

La sentencia del TCF sobre el censo (*Volkszählungsurteil*) de 1983 constituye un hito fundamental en el constitucionalismo global de la privacidad. El fallo del TCF, al revisar la constitucionalidad del censo nacional en 1983, reconoció por primera vez un "*Recht auf informationelle Selbstbestimmung*" (derecho a la autodeterminación informacional) como derecho fundamental autónomo. La sentencia estableció que, bajo condiciones modernas de procesamiento de datos, la protección de la personalidad requiere capacidad del individuo para determinar divulgación y uso de datos personales. El Tribunal articuló los principios fundamentales de consentimiento informado, limitación o vinculación a un propósito (*Zweckbindung*), proporcionalidad en recolección de datos, y transparencia en tratamiento. Esta conceptualización influyó decisivamente en la Directiva europea 95/46/CE y el actual RGPD, estableciendo a Alemania como líder mundial en protección constitucional de datos[23].

Adaptación a la era digital

La sentencia del TCF en el caso de Investigación en línea (*Online-Durchsuchungs-Urteil*) (2008) mostró la capacidad adaptativa del constitucionalismo alemán ante ciertos desafíos tecnológicos. El Tribunal reconoció el derecho fundamental a garantía de confidencialidad e integridad de sistemas informáticos ("*Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*"), adaptando así la protección constitucional a la era digital. Esta innovación jurisprudencial protege los sistemas informáticos como una extensión de la personalidad, estableciendo la confidencialidad de datos almacenados e integridad contra la manipulación, con limitaciones estrictas para la intervención estatal. Casos posteriores sobre derecho al olvido (2019) equilibraron la protección a la personalidad con la libertad de expresión en contextos digitales, desarrollando criterios de paso del tiempo, relevancia actual de información, posición pública del afectado, y gravedad de la conducta pasada.

[23] Simitis (1987:707).

4. Marco legislativo de la protección de datos

Alemania desarrolló un marco legislativo integral en materia de protección de datos, comenzando con la Ley federal de Protección de Datos (*Bundesdatenschutzgesetz*, BDSG) de 1977. Reformas posteriores (1990, 2001) han adaptado la normativa a directivas europeas y la evolución tecnológica. El nuevo BDSG de 2018 implementó el RGPD en el derecho alemán. El sistema federal alemán incluye autoridades de protección de datos en los estados federados (*Länder*), creando una estructura descentralizada pero coordinada. El encargado Federal para la protección de datos y la libertad de información (*Bundesbeauftragter für den Datenschutz und die Informationsfreihei*t, BfDI) actúa como autoridad federal con independencia constitucional, supervisando el cumplimiento normativo y ejerciendo potestad sancionadora.

5. Influencia global del modelo alemán

El modelo alemán de autodeterminación informacional ha ejercido una influencia global excepcional. Conceptos desarrollados en la sentencia sobre el censo (consentimiento informado, vinculación de propósito, proporcionalidad, transparencia) constituyen pilares del derecho europeo de protección de datos y han sido adoptados en múltiples jurisdicciones. El RGPD incorpora estos principios como estándar europeo, creando lo que se conoce como "efecto Bruselas", que extiende la influencia alemana globalmente. Países latinoamericanos, asiáticos y africanos han adoptado elementos del modelo alemán en legislaciones nacionales.

V. España: protección integral y carácter pionero en lo digital

6. Contexto de la transición democrática y Constitución de 1978

La Constitución española de 1978 emerge del consenso democrático post-franquista, incorporando desarrollos constitucionales europeos contemporáneos en un marco de protección amplia de derechos fundamentales. El artículo 18 establece un sistema integral de protección a la privacidad sin precedentes históricos: honor, intimidad personal y familiar, propia imagen (18.1), inviolabilidad domiciliar (18.2), secreto de comunicaciones (18.3), y

limitación del uso de informática (18.4). Esta última disposición convierte a España en la primera constitución mundial en mencionar explícitamente la informática, anticipando desafíos de la era digital con notable visión prospectiva. El modelo español integra influencias del constitucionalismo alemán, italiano y del Convenio Europeo de Derechos Humanos, creando una síntesis original que combina tradición continental con innovación tecnológica[24].

7. Desarrollo jurisprudencial del Tribunal Constitucional

La jurisprudencia del Tribunal Constitucional español, en adelante TCE, ha desarrollado sistemáticamente el contenido del artículo 18 Constitución Española. La sentencia del Tribunal Constitucional, sucesivamente STC, identificada como STC 89/1987 (Caso Violeta Friedman) estableció la primera definición constitucional de intimidad como "esfera reservada de la persona y su familia", desarrollando un criterio de relevancia pública versus interés privado para su ponderación con la libertad de expresión. La STC 134/1999 (Caso Paquirri) configuró definitivamente el derecho a la imagen, estableciendo su carácter personalísimo, transmisibilidad mortis causa limitada, y criterios de ponderación con libertad de información basados en relevancia pública. La STC 292/2000 constituyó un hito en la interpretación del artículo 18.4, reconociendo la "libertad informática" como derecho autónomo que incluye los derechos de no ser fichado, a acceso, de rectificación y cancelación. Esta jurisprudencia estableció las bases conceptuales para el desarrollo legislativo posterior en material de protección de datos.

8. Evolución Legislativa en Protección de Datos

España desarrolló un marco legislativo pionero en protección de datos. La Ley Orgánica -LO 1/1982 de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, concretó el artículo 18.1, definiendo las hipótesis de intromisiones ilegítimas y estableciendo acciones de protección en el ámbito civil. La Ley Orgánica de Protección de Datos o LOPD (LO 15/1999 de 13 de diciembre) aplicó la Directiva 95/46/CE, estableciendo los principios de consentimiento, calidad de datos, finalidad específica y proporcionalidad, junto con derechos ARCO (Acceso, Rectificación, Cancelación, Oposición). La creación de la Agencia Española de Protección de Datos AEPD (1992) como primera autoridad de protección de datos a nivel mundial, demostró el liderazgo español en la institucionalización de la protección de datos. La LO 3/2018 de 5 de diciembre

[24] Pérez Luño (2018:323 y ss.).

de protección de datos personales y garantías de derechos digitales adaptó derecho español al RGPD, introduciendo innovaciones significativas en el Título X "Garantía de derechos digitales", asumiendo nuevamente un carácter pionero a nivel mundial, esta vez en el reconocimiento legislativo de derechos específicos de la era digital: el derecho a la desconexión digital, la intimidad digital, el derecho al olvido, a la portabilidad y al testamento digital. Esta normativa ubicó a España como referencia global en regulación de derechos digitales.

9. Desafíos y Tensiones Contemporáneas

El sistema español de protección de privacidad enfrenta desafíos múltiples durante el 2025. Tecnológicamente, la inteligencia artificial, el Internet de las Cosas y modelos de negocio basados en datos personales presionan marcos normativos existentes. La Agencia ha adoptado un enfoque proactivo, desarrollando guías sobre inteligencia artificial (IA), reconocimiento facial, y cookies, posicionando a España como líder en aplicación práctica del RGPD. Socialmente, la tensión entre privacidad y transparencia se manifiesta en conflictos entre derecho al olvido y libertad de información, los que se han venido solucionando con una ponderación casuística. Políticamente, los debates sobre la vigilancia estatal post-COVID y seguridad nacional versus derechos digitales se mantienen vigentes. La integración de la jurisprudencia europea con la doctrina constitucional española presenta complejidades interpretativas. El modelo español de derechos digitales (LO 3/2018) está siendo observado internacionalmente como posible referencia para actualización de marcos normativos nacionales.

VI. Chile

1. Contexto Constitucional e Histórico

La Constitución chilena de 1980, en su artículo 19 N°4 garantiza "El respeto y protección a la vida privada y a la honra de la persona y su familia", mientras su N°5 protege "La inviolabilidad del hogar y de toda forma de comunicación privada". Esta formulación, influida por el constitucionalismo clásico, carece de referencias específicas a desafíos informacionales o tecnológicos, requiriendo interpretación judicial expansiva para adaptarse a realidades contemporáneas. La transición democrática (1990) mantuvo

el texto constitucional, aunque reformas posteriores (especialmente 2005) modernizaron otros aspectos. El debate constituyente 2019-2022, aunque fracasado, evidenció la desactualización de derechos digitales y protección de datos en marco constitucional.

2. Desarrollo jurisprudencial nacional

La jurisprudencia chilena ha desarrollado el contenido de la protección a la vida privada principalmente a través de fallos del Tribunal Constitucional (TC) y Corte Suprema (CS). La sentencia del TC rol N° 389-2003 estableció una primera definición constitucional de la vida privada como "esfera de intimidad personal exenta de intromisiones", desarrollando un test de proporcionalidad entre fin público y afectación de privacidad. El fallo del TC Rol N° 1683-2010 adaptó la protección de las comunicaciones a la era digital, estableciendo principios de reserva legal estricta, proporcionalidad, control judicial previo y limitación temporal para interceptaciones. La sentencia del TC Rol N°2388-2012 conectó vida privada con protección de datos en el contexto de archivos de inteligencia, reconociendo la dimensión informacional de la privacidad. Por su parte, la CS ha desarrollado su doctrina mediante recursos de protección, estableciendo en el fallo de la CS Rol N°25625-2019 criterios para el derecho al olvido (aun en ausencia de ley), equilibrando la privacidad con libertad de información mediante factores de relevancia pública, paso del tiempo, exactitud y daño personal.

3. Marco legislativo de protección de datos

La Ley 19.628 (1999) constituyó la primera ley comprensiva de protección de vida privada en Chile, estableciendo principios de licitud, finalidad específica, consentimiento y calidad de información para tratamiento de datos personales. La ley incluye derechos de información, acceso, rectificación y eliminación, aplicables a sectores público y privado. Sin embargo, carece de una autoridad de control independiente y presenta sanciones limitadas, evidenciando desactualización frente a estándares internacionales contemporáneos. La Ley 20.285 (2008) sobre acceso a información pública buscó establecer un equilibrio entre transparencia y protección de vida privada, creando el Consejo para la Transparencia como autoridad especializada. La Ley 21.719 modernizó el marco inspirándose en el RGPD, incluyendo la creación de una autoridad de protección de datos, sanciones administrativas, derechos ampliados y principio de *accountability* empresarial.

Matriz Comparativa de Sistemas Constitucionales de Privacidad

Dimensión	Estados Unidos	Alemania	España	Chile
Fundamento Constitucional	4ª y 14ª Enmiendas (implícito)	Arts. 1(1) y 2(1) GG	Artículo 18 CE (expreso)	Artículo 19 N°4 y N°5 CPR
Categorías Reconocidas	Decisional, espacial	Informacional, personalidad	Integral (honor, intimidad, imagen, datos)	Vida privada, honra, comunicaciones
Estándares Jurisprudenciales	Expectativa razonable, escrutinio estricto	Ponderación, proporcionalidad	Ponderación, relevancia pública	Proporcionalidad, arbitrariedad
Autoridades de Control	Sectoriales (FTC, HHS, etc.)	BfDI (federal) + *Länder*	AEPD (independiente)	Ninguna especializada
Remedios Principales	Revisión judicial, § 1983	Recurso constitucional	Recurso de amparo, acción civil	Recurso de protección
Influencias Externas	Limitadas	CEDH, derecho UE	CEDH, TJUE, RGPD	CADH, Corte IDH
Desafíos Actuales (2025)	Fragmentación post-Dobbs, ausencia marco federal datos	IA, equilibrio innovación-protección	Implementación derechos digitales	Modernización normativa urgente

Fuente:

Elaboración propia basada en investigación jurisprudencial y normativa.

Capitulo 2
Evolución normativa sobre datos personales a nivel europeo, latinoamericano y nacional[25]

El derecho al respeto de la vida privada y el derecho a la protección de los datos personales son derechos distintos, aunque se relacionan. El derecho a la privacidad o vida privada surge en la Declaración Universal de Derechos Humanos (DUDH), adoptada en 1948. Con posterioridad los sistemas regionales también lo han ido reconociendo a través de sus propios instrumentos, como son la Convención Americana de Derechos Humanos -CADH- y la Convención Europea de Derechos Humanos -CEDH- las que reconocen que las personas tienen derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

Naturalmente, los instrumentos internacionales vinculantes referidos son precedentes al arribo de la revolución tecnológica computacional, internet y sociedad de la información y comunicación que se vivencia hoy. Estos adelantos que han generado ventajas para la población y las comunidades, mejorando en muchos casos la calidad de vida, también han generado inéditos desafíos ante el respeto de la vida privada, que arriesga ser vulnerada. Entonces, como una necesidad de dar respuesta a la protección del derecho a la vida privada y contar con normativas que regulasen los eventuales riesgos/vulneraciones/amenazas/etc. que se pueden ocasionar por la recopilación y uso de la información personal nace el concepto de "privacidad", "privacidad de la información" o "derecho a la autodeterminación informacional". La creación de este vocablo dio un espacio a la generación paulatina de un estatuto de protección de datos personales.

En este sentido, se presentan algunos de los principales ejes del "*Handbook on European Data Protection Law*"[26], estableciendo conexiones con la evolución latinoamericana y chilena. A partir de un enfoque comparado, se propone una lectura sistemática de los principios, derechos, instituciones y desafíos que caracterizan la arquitectura europea, con especial atención a su irradiación normativa hacia América Latina.

[25] Este análisis se basa principalmente en el Handbook on European Data Protection Law (FRA et al., 2018).

[26] FRA et al. (2018:15–92).

I. Antecedentes generales del modelo europeo

El surgimiento del derecho a la protección de datos personales se vincula con la reconstrucción del Estado de derecho tras la Segunda Guerra Mundial y con la necesidad de limitar el poder informacional del Estado.

El Convenio 108 del Consejo de Europa (1981) se erige como el primer tratado internacional vinculante que regula el tratamiento automatizado de datos personales, reconociendo el principio de control individual sobre la información.[27] Todos los Estados miembros de la Unión Europea han ratificado el Convenio 108. Durante el año 1999 se modifica el Convenio 108 para que la UE pudiera ser Parte del mismo.[28] En el año 2001 se adoptó un Protocolo Adicional al Convenio 108, que introdujo disposiciones sobre los flujos de datos transfronterizos a los Estados no Partes o los terceros países, sobre la obligatoriedad de crear autoridades nacionales de control de protección de los datos. Actualmente, participan 46 Estados miembros del Consejo de Europa, así como Argentina, Cabo Verde, Marruecos, Mauricio, México, Senegal, Túnez y Uruguay. El convenio se sometió a un proceso de modernización entre el 2011 y 2018, resultando un potencial instrumento universal de protección de datos. Se refuerza y consolidan principios importantes y confiere nuevos derechos a las personas físicas, al tiempo que aumenta las responsabilidades de las entidades que tratan datos personales y garantiza una mayor rendición de cuentas.

Posteriormente, la Directiva 95/46/CE de la UE (un reglamento) sirvió para robustecer un enfoque basado en la protección de derechos fundamentales, anticipando el reconocimiento del derecho autónomo a la protección de datos en la Carta de Derechos Fundamentales de la Unión Europea (artículo 8). Se adoptó en 1995, cuando ya varios países habían incorporado leyes nacionales de protección de datos.[29] Uno de los objetivos fue armonizar legislaciones para garantizar un elevado nivel de protección y la libre circulación de datos

[27] FRA et al. (2018:25–28).

[28] Consejo de Europa, Modificaciones del Convenio para la protección de las personas en relación con el tratamiento automatizado de datos de carácter personal (STCE n.o)108) para permitir la adhesión de las Comunidades Europeas, adoptado por el Comité de Ministros el 15 de junio de 1999 en Estrasburgo; artículo)23, apartado)2, del Convenio)108 en su versión modificada.

[29] El estado alemán de *Hesse* adoptó la primera ley del mundo sobre protección de datos en 1970, que solo se aplicaba en ese estado. Suecia adoptó la *Datalagen* en 1973; Alemania la *Bundesdatenschutzgestez* en 1976; y Francia la *Loi relative à l'informatique, aux fichiers et aux libertés* en 1977. En el Reino Unido, la *Data Protection Act* se adoptó en 1984. Por último, los Países Bajos adoptaron los *Wet Persoonregistraties* en 1989.

personales entre los diferentes Estados miembros. La libre circulación de bienes y servicios/ capitales y personas en el mercado, requieren una libre circulación de datos, pero ella no puede ocurrir en contextos de desconfianza respecto de su adecuada protección. Es decir, habría un tránsito desde la privacidad hacia la autodeterminación informativa, inspirado en la doctrina alemana de los años setenta.[30]

La **independencia institucional de las autoridades de control** constituye uno de los pilares estructurales del sistema europeo de protección de datos personales y una garantía indispensable para la tutela efectiva del derecho a la autodeterminación informativa. Dicha independencia no se concibe únicamente como separación formal del poder político o de los sujetos regulados, sino como una **autonomía funcional y técnica integral**, que asegure la imparcialidad y continuidad del control.[31]

En el marco del **artículo 52 del RGPD,**[32] las autoridades nacionales de control deben contar con **recursos humanos, técnicos y financieros suficientes**, así como con **competencias propias de investigación, corrección y sanción**, incluyendo la potestad de imponer multas administrativas significativas y de ordenar la suspensión o modificación de tratamientos de datos ilícitos. Este diseño institucional se orienta a garantizar una supervisión eficaz y disuasiva, equiparable en jerarquía a la de un órgano constitucionalmente autónomo.

A nivel supranacional, el **Comité Europeo de Protección de Datos** (*European Data Protection Board*, **EDPB**) ejerce un rol de **coherencia y**

[30] En este punto hay una diferencia con la legislación norteamericana, que se caracteriza por regular los datos personales desde la autorregulación y responsabilidad contractual.

[31] FRA et al. (2018:52–60).

[32] Artículo 52: Asimismo deben autorizarse excepciones a la prohibición de tratar categorías especiales de datos personales cuando lo establezca el Derecho de la Unión o de los Estados miembros y siempre que se den las garantías apropiadas, a fin de proteger datos personales y otros derechos fundamentales, cuando sea en interés público, en particular el tratamiento de datos personales en el ámbito de la legislación laboral, la legislación sobre protección social, incluidas las pensiones y con fines de seguridad, supervisión y alerta sanitaria, la prevención o control de enfermedades transmisibles y otras amenazas graves para la salud. Tal excepción es posible para fines en el ámbito de la salud, incluidas la sanidad pública y la gestión de los servicios de asistencia sanitaria, especialmente con el fin de garantizar la calidad y la rentabilidad de los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro de enfermedad, o con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos. Debe autorizarse asimismo a título excepcional el tratamiento de dichos datos personales cuando sea necesario para la formulación, el ejercicio o la defensa de reclamaciones, ya sea por un procedimiento judicial o un procedimiento administrativo o extrajudicial.

armonización interpretativa, asegurando la aplicación uniforme del RGPD en todos los Estados miembros. Dicho Comité —integrado por los representantes de las autoridades nacionales y el Supervisor Europeo de Protección de Datos— emite **directrices, recomendaciones y decisiones vinculantes**, contribuyendo a la **unidad jurisprudencial y administrativa** del espacio europeo de protección de datos.

El régimen europeo de transferencias internacionales de datos personales se erige sobre el principio de adecuación sustancial del nivel de protección, conforme al cual los datos sólo pueden ser transferidos a terceros países o destinatarios internacionales que aseguren garantías equivalentes a las previstas por el ordenamiento de la UE. Este principio, previsto en los artículos 44 a 50 del RGPD, busca preservar la unidad del estándar de tutela y evitar que la salida transfronteriza de datos se convierta en una forma de eludir las obligaciones impuestas dentro del Espacio Económico Europeo.

El mecanismo de adecuación —formalizado mediante decisiones adoptadas por la Comisión Europea— exige una evaluación exhaustiva del marco normativo, institucional y judicial del país receptor, verificando la existencia de normas vinculantes, recursos efectivos y órganos de supervisión independientes. Solo en presencia de este nivel de protección "sustancialmente equivalente" puede autorizarse la transferencia sin requisitos adicionales.

Este modelo ha sido perfeccionado y constitucionalizado a través de la jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE), particularmente en los casos *Schrems I* (C-362/14, 2015) y *Schrems II* (C-311/18, 2020). En ambos pronunciamientos, el Tribunal invalidó los acuerdos internacionales "*Safe Harbor*" y "*Privacy Shield*", al estimar que no ofrecían un nivel de protección equiparable al exigido por el Derecho de la Unión, especialmente frente a la injerencia de autoridades públicas en la vigilancia masiva de datos. Tales decisiones consolidaron la noción de equivalencia sustancial como parámetro constitucional europeo y reafirmaron la competencia del TJUE para controlar la validez de los regímenes de transferencia.

En ausencia de una decisión de adecuación, el RGPD prevé mecanismos complementarios de garantía, como las cláusulas contractuales tipo, las normas corporativas vinculantes (*Binding Corporate Rules*) o, excepcionalmente, determinadas situaciones de interés público o consentimiento explícito del titular. Todos estos instrumentos responden a una lógica de responsabilidad proactiva y extraterritorial, en virtud de la cual el responsable del tratamiento mantiene su deber de diligencia sobre los datos incluso más allá del territorio de la Unión.

Desde una perspectiva comparada, este modelo de extraterritorialidad normativa y de equivalencia sustancial ha ejercido una influencia decisiva en los procesos de reforma latinoamericanos.

II. Antecedentes generales del modelo latinoamericano y chileno

La configuración del derecho a la protección de datos personales en América Latina se desarrolló en un contexto distinto al europeo, marcado por transiciones democráticas, procesos constituyentes y la consolidación del constitucionalismo de los derechos. A diferencia del modelo europeo —basado en la integración supranacional y en instrumentos normativos uniformes—, la tradición latinoamericana evolucionó desde el derecho a la privacidad hacia la autodeterminación informativa, a través de una vía constitucional y jurisprudencial, en la que el juez desempeñó un rol decisivo en la construcción de garantías frente al poder informacional del Estado y de los particulares.

El punto de partida regional fue la incorporación del *Hábeas data* como acción constitucional autónoma, concebida como una herramienta procesal de acceso, rectificación y supresión de información personal contenida en registros públicos o privados. El reconocimiento de los derechos de los titulares de datos personales constituye el eje sustantivo del sistema de protección de datos, en cuanto mecanismo que materializa la autodeterminación informativa. Esto se llevó a cabo generalmente bajo el modelo ARCO y en los últimos años, las legislaciones más avanzadas han ampliado este catálogo, incorporando derechos complementarios como la portabilidad, la limitación del tratamiento y la oposición a decisiones automatizadas, en consonancia con el estándar europeo.

La tutela de estos derechos se ha ejercido principalmente mediante el *Hábeas data*, acción constitucional que permite al titular acceder, rectificar o suprimir información errónea o ilegítimamente tratada. No obstante, el diseño procesal del *Hábeas data* —por su naturaleza correctiva y su dependencia de la iniciativa individual— ha demostrado limitaciones estructurales: dispersión jurisprudencial, falta de órganos técnicos de apoyo y escasa capacidad de supervisión ex ante. Así, pese a su eficacia simbólica y su arraigo constitucional, el modelo no posee una efectividad preventiva, especialmente frente a tratamientos masivos y automatizados de datos.

Su origen se remonta a la Constitución de Brasil de 1988 (artículo 5, LXXII), que inauguró la tendencia regional de vincular el control de la información con el debido proceso y la dignidad humana. Posteriormente, Colombia (1991, artículo 15), Paraguay (1992, artículo 135), Perú (1993, artículo 200.3) y Argentina (1994, artículo 43) constitucionalizaron la figura, dotándola de una eficacia directa ante los tribunales constitucionales o de amparo. Al igual que en Europa, el *Hábeas data* cumplió una función eminentemente reactiva, dirigida a corregir o eliminar registros inexactos, discriminatorios o ilegítimos. Sin embargo, su interpretación jurisprudencial —particularmente en Colombia, Argentina y Brasil— permitió dotarlo de un contenido sustantivo, transformándolo en un instrumento de control activo del flujo informacional. Esta evolución interpretativa condujo a la identificación de un derecho fundamental autónomo de la protección de datos personales.

Durante las décadas de 1990 y 2000, la región avanzó hacia la adopción de leyes generales de protección de datos personales, inspiradas en las Directrices de la OCDE (1980) y, en menor medida, en la Directiva 95/46/CE de la Unión Europea. La Ley Argentina 25.326 (2000) inauguró este proceso, constituyéndose en la primera normativa integral del continente y obteniendo en 2003 una decisión de adecuación por parte de la Comisión Europea. Le siguieron Uruguay (Ley 18.331, 2008) -reconocida como país adecuado en 2012- , México (Ley Federal de Protección de Datos Personales en Posesión de los Particulares, 2010), Perú (Ley 29.733, 2011), Colombia (Ley Estatutaria 1581, 2012) y Brasil (*Lei Geral de Proteção de Dados Pessoais*, 13.709, 2018).

Estas normas reflejan una aproximación convergente hacia los principios estructurales del modelo europeo —licitud, finalidad, proporcionalidad, calidad, seguridad y consentimiento informado—, pero enmarcados en sistemas institucionales heterogéneos. En algunos países, la supervisión corresponde a las autoridades administrativas especializadas con autonomía técnica, y en otros, la tutela recae en tribunales constitucionales o jueces de amparo, mediante acciones directas. Este diseño híbrido evidencia una asimetría institucional, que, no obstante, ha permitido consolidar progresivamente un bloque latinoamericano de protección de datos con estándares cada vez más uniformes.

Por otro lado, la jurisprudencia de la Corte Interamericana de Derechos Humanos ha contribuido a dotar al modelo latinoamericano de una densidad jurídica propia. A partir del artículo 11 de la Convención Americana sobre Derechos Humanos, la Corte ha interpretado la protección de los datos personales como una dimensión autónoma del derecho a la vida privada. En

Escher y otros vs. Brasil (2009), se afirmó que los Estados tienen la obligación positiva de garantizar la confidencialidad y la legalidad del tratamiento de información personal. En *Tristán Donoso vs. Panamá* (2009) y *Gomes Lund y otros vs. Brasil* (2010), se reafirmó la relación entre privacidad, libertad de expresión y acceso a la información, estableciendo un estándar regional que vincula el control informacional con el principio de proporcionalidad y con el deber de rendición de cuentas estatal.

Desde el plano doctrinal, el modelo latinoamericano ha ido asimilando la noción de autodeterminación informativa como categoría jurídica sustantiva, entendida como la facultad de toda persona para decidir sobre la recolección, uso y destino de sus datos personales. Esta concepción, derivada del pensamiento constitucional alemán y español, ha sido adaptada al contexto latinoamericano como un instrumento de control democrático del poder informacional, orientado tanto al Estado como a los agentes privados. La información deja de ser un objeto de privacidad para convertirse en una manifestación de la identidad personal y del principio de igualdad material, especialmente frente a los riesgos de exclusión digital y perfilamiento automatizado.

En la última década, América Latina ha ingresado en una etapa de madurez normativa y cooperación institucional, marcada por la creación de la Red Iberoamericana de Protección de Datos (RIPD) y por la adopción de los Principios sobre Privacidad y Protección de Datos Personales de la OEA (2015). Estos instrumentos promueven la armonización legislativa y la adopción de estándares comunes basados en la transparencia, la proporcionalidad y la responsabilidad proactiva, aproximándose la región al paradigma europeo de gobernanza digital.

La Ley chilena 21.719 constituye un punto de inflexión en este proceso, creando una Agencia con autonomía técnica y potestades sancionatorias y estableciendo un régimen de transferencias internacionales, evaluaciones de impacto y sanciones administrativas coherentes con el RGPD. Este paso sitúa a Chile dentro del grupo de Estados que aspiran a obtener una decisión de adecuación por parte de la Unión Europea, fortaleciendo su inserción en los flujos digitales globales bajo un enfoque de protección de derechos.

El modelo latinoamericano, en su actual fase de consolidación, demanda del juez una comprensión dinámica del derecho a la protección de datos como derecho operativo y de aplicación directa, dotado de eficacia transversal sobre todas las ramas del ordenamiento jurídico. Ello implica evaluar, en cada caso, la proporcionalidad del tratamiento, la legitimidad del consentimiento, la finalidad específica del uso de los datos y la existencia de

garantías efectivas frente a su circulación transfronteriza. En este sentido, la función judicial no se limita al control de legalidad, sino que se proyecta como una garantía institucional del equilibrio entre innovación tecnológica, libertad informacional y dignidad humana.

Con la modificación legal se consagran acciones de tutela directa ante la Agencia, dotándola de potestades correctivas, orientadoras y sancionatorias, sin excluir la revisión judicial posterior. El responsable del tratamiento debe acreditar que toda operación sobre datos se ajusta a los principios establecidos en la norma.

De este modo, el modelo latinoamericano contemporáneo transita hacia una tutela multinivel, en que la protección judicial se complementa con la fiscalización administrativa especializada y con obligaciones de cumplimiento preventivo. La función judicial, en este escenario, exige evaluar no solo la existencia de un daño o infracción, sino también la suficiencia de las medidas de diligencia y de gestión de riesgos adoptadas por el responsable del tratamiento, conforme a los estándares de buena administración de datos y protección reforzada de los derechos fundamentales.

Con respecto a la independencia y eficacia de las autoridades de control en América Latina, la institucionalidad ha seguido un camino evolutivo más desigual, donde coexisten estructuras altamente desarrolladas con otras aún dependientes de ministerios o subsecretarías, lo que repercute en la capacidad sancionatoria y en la confianza pública. En el plano comparado, Uruguay, México y Brasil representan los modelos más consolidados. En Uruguay, la Unidad Reguladora y de Control de Datos Personales (URCDP) ejerce potestades de supervisión y sanción con independencia administrativa; en México, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) coordina la doble función de transparencia pública y privacidad individual; y en Brasil, la *Autoridade Nacional de Proteção de Dados* (ANPD) actúa como órgano técnico autónomo, con atribuciones para fiscalizar, dictar directrices y sancionar infracciones graves.

Sin embargo, en otros Estados de la región persisten modelos dependientes del Poder Ejecutivo, sin autonomía decisoria ni estabilidad presupuestaria, lo que compromete su efectividad y dificulta la cooperación internacional. Esta disparidad institucional fragmenta la capacidad de respuesta frente a incidentes transfronterizos y debilita los mecanismos de cumplimiento coordinado.

La Ley 21.719 se alinea con un diseño exigente al crear la Agencia con rango de órgano autónomo y facultades amplias: instrucción de procedimientos sancionatorios, dictación de directrices interpretativas, aprobación

de códigos de conducta, auditorías y evaluaciones de impacto. Este diseño responde al principio de control independiente y a la necesidad de dotar al sistema nacional de legitimidad ante los marcos internacionales de intercambio de datos. En la práctica judicial, ello implica que las resoluciones y directrices de la Agencia constituirán referentes interpretativos relevantes para el control de legalidad y proporcionalidad del tratamiento de datos en sede jurisdiccional.

En cuanto a la cooperación internacional, la participación activa de los países latinoamericanos en la RIPD y en los Principios de la OEA sobre Privacidad (2015) favorece la convergencia técnica, el intercambio de buenas prácticas y la armonización de estándares regionales, fortaleciendo la posición de la región en los foros multilaterales (OCDE, Consejo de Europa, ONU).

En cuanto a la transferencia transfronteriza de datos personales se plantea un desafío jurídico de alta complejidad: el de compatibilizar la libre circulación económica con la preservación del nivel esencial de protección de los derechos fundamentales. En el modelo europeo, el principio de adecuación sustancial constituye la piedra angular de este equilibrio, al establecer que solo podrán transferirse datos hacia países que ofrezcan garantías equivalentes a las del RGPD. Este control ex ante tiene por finalidad evitar que la exportación de datos se traduzca en una elusión del marco protector europeo. El mecanismo de adecuación, formalizado mediante decisiones de la Comisión Europea, evalúa de manera integral el marco normativo, institucional y jurisdiccional del país receptor.

La Ley 21.719 incorpora un modelo inspirado en estos estándares, imponiendo la obligación de evaluación de riesgos en transferencias internacionales y la verificación de garantías adecuadas mediante instrumentos como las cláusulas contractuales tipo, las normas corporativas vinculantes o el reconocimiento de decisiones de adecuación extranjeras. Además, exige que toda transferencia se funde en un interés legítimo y proporcional, garantizando el respeto del principio de finalidad y la continuidad del control sobre el dato transferido.

Este enfoque refleja una lógica de responsabilidad extraterritorial, conforme a la cual el responsable del tratamiento mantiene el deber de diligencia sobre los datos aun fuera de la jurisdicción nacional. En la práctica judicial, ello implica que la transferencia internacional no exime de responsabilidad al controlador original, quien debe acreditar la existencia de garantías adecuadas y mecanismos de reparación efectivos.

Finalmente, el fortalecimiento de la cooperación transnacional y la convergencia con los estándares europeos constituyen elementos estratégicos para la consolidación de un estatuto de protección de datos.

III. Desafíos contemporáneos: inteligencia artificial, vigilancia y derechos digitales

El advenimiento de la inteligencia artificial (IA), la biometría avanzada y el *big data* ha transformado radicalmente las condiciones en que se recolecta, procesa y utiliza la información personal, planteando nuevos desafíos para el derecho de protección de datos y, en particular, para el rol judicial en la tutela de los derechos digitales. Estas tecnologías amplifican las capacidades de predicción, perfilamiento y decisión automatizada, incrementando los riesgos de discriminación algorítmica, vigilancia masiva y opacidad en la toma de decisiones públicas y privadas.

En el sistema europeo, la respuesta jurídica se ha articulado sobre los principios de intervención humana significativa, proporcionalidad y evaluación de impacto en la protección de datos. El artículo 22 del RGPD prohíbe, como regla general, que una persona sea objeto de una decisión basada exclusivamente en el tratamiento automatizado de datos, incluida la elaboración de perfiles, cuando dicha decisión produzca efectos jurídicos o afecte significativamente al individuo. Este precepto —complementado por las directrices del Comité Europeo de Protección de Datos (EDPB)— consagra la exigencia de que toda decisión automatizada relevante sea susceptible de revisión humana, garantizando el derecho a la explicación y la corrección de sesgos sistémicos.

El principio de proporcionalidad y la evaluación de impacto de protección de datos (*Data Protection Impact Assessment*, DPIA) son herramientas esenciales de gobernanza algorítmica.[33] Estas permiten anticipar y mitigar riesgos antes de la implementación de sistemas automatizados, asegurando la compatibilidad entre la innovación tecnológica y la protección efectiva de los derechos fundamentales. En el plano institucional, la UE avanza hacia la consolidación del Reglamento 24/1689 de 13 de junio, sobre Inteligencia Artificial.

[33] FRA et al. (2018:85–89).

Para los jueces latinoamericanos, y en particular para la judicatura chilena, el desafío reside en compatibilizar la innovación tecnológica con la tutela judicial efectiva de los derechos fundamentales en entornos digitales. Ello exige interpretar las normas de protección de datos, privacidad y debido proceso desde una perspectiva proactiva y de control de legalidad tecnológica, verificando que los sistemas de decisión automatizada respeten los principios de transparencia, necesidad y proporcionalidad, y que la persona mantenga una posición central de autonomía frente al poder informacional.

En sociedades caracterizadas por brechas tecnológicas y regulatorias, como las latinoamericanas, la consolidación de un marco de protección adecuado requerirá no solo de legislación especializada, sino también de una cultura judicial de derechos digitales, capaz de garantizar que el uso de la IA y del *big data* se someta a los mismos estándares de legalidad, control y rendición de cuentas que rigen las demás actuaciones del poder público y privado.

IV. Cuadro comparativo. Síntesis analítica

El siguiente cuadro presenta un análisis comparado del derecho a la autodeterminación informativa en Europa, América Latina y Chile, considerando su evolución doctrinal, desarrollo normativo y situación actual al año 2026.

Eje de comparación	Europa (Unión Europea y Consejo de Europa)	América Latina	Chile
Fundamento constitucional y filosófico	Deriva del principio de dignidad humana (artículo 1 Carta de Derechos Fundamentales de la UE) y del derecho a la vida privada (artículo 8 CEDH). Se consolida con la jurisprudencia del Tribunal Constitucional Federal Alemán (Caso del Censo, 1983), que acuña el concepto de autodeterminación informativa.	Inspirado por el modelo europeo continental, especialmente el alemán y el español. Se articula en torno al derecho a la intimidad, al *Hábeas data* y al control del uso de la información personal.	Reconocido a partir del artículo 19 N°4 y N°5 de la Constitución, desarrollado por la Ley 19.628 (1999) y la Ley 21.719 (2024), que adapta los estándares del RGPD.

Reconocimiento explícito del derecho	Artículo 8 de la Carta de Derechos Fundamentales de la UE. RGPD (2016/679) desarrolla derechos como acceso, rectificación, portabilidad, supresión y oposición.	Constituciones de Argentina, Brasil, Colombia, México y Perú. Existen leyes nacionales inspiradas en el RGPD o en las Directrices de la OEA y OCDE.	La Ley 21.719 (2024) reconoce el derecho a la autodeterminación informativa como fundamental, crea la Agencia y regula principios como finalidad, minimización y consentimiento informado.
Autoridad de control y mecanismos institucionales	Autoridades nacionales de control (*Data Protection Authorities*), coordinadas por el Comité Europeo de Protección de Datos (EDPB).	Modelos diversos: autoridades autónomas (INAI, ANPD, AAIP) o defensorías del pueblo. Proceso de europeización institucional.	Creación de la Agencia como ente autónomo, con facultades sancionatorias y fiscalizadoras.
Ámbito de aplicación	Sector público y privado. Aplicación extraterritorial (artículo 3 RGPD). Protección integral frente a actores digitales globales.	Predomina la protección mixta. Algunos países excluyen parcialmente el ámbito privado o los datos de seguridad nacional.	Aplicación general a todos los tratamientos de datos, públicos y privados, con sanciones administrativas y civiles.
Principios rectores	Licitud, lealtad y transparencia; limitación de finalidad; minimización; exactitud; integridad y confidencialidad; responsabilidad proactiva.	Similares a los principios europeos, con énfasis en consentimiento informado, finalidad legítima y seguridad de la información.	Licitud, transparencia, minimización, responsabilidad y seguridad. Protección reforzada de datos sensibles y creación del Delegado de Protección de Datos.
Derechos de las personas	Acceso, rectificación, supresión (derecho al olvido), limitación, portabilidad, oposición, no ser objeto de decisiones automatizadas.	Acceso, rectificación, actualización, cancelación y oposición (modelo ARCO). Algunos países añaden derecho al olvido.	Derechos ARCO+, incluyendo portabilidad, oposición, supresión y protección frente a decisiones automatizadas.
Responsabilidad y sanciones	Sanciones hasta el 4% del volumen global de negocios (RGPD). Responsabilidad objetiva y solidaria entre controlador y encargado.	Multas variables y mecanismos judiciales (*Hábeas data*, amparo). En Brasil, sanciones administrativas; en Colombia y Argentina, tutela judicial.	Sanciones administrativas (hasta 10.000 UTM), responsabilidad civil y acción constitucional directa ante tribunales.
Doctrina dominante	Concepción del dato como proyección de la personalidad. El individuo es titular de su identidad informacional (Habermas, Simitis, González Fuster).	Predomina la visión de derecho a la privacidad reforzada, como instrumento de control sobre Estado y mercados digitales.	Se consolida la idea de autodeterminación informativa como manifestación de la dignidad humana. Jurisprudencia chilena reciente. Ej. Corte Suprema, Tercera Sala, 6 de enero de 2025 (causa Rol N.º 18.566-2024); Corte Suprema (13 mayo 2025), Recurso de protección contra Destácame SpA

Tendencias actuales	Gobernanza algorítmica, ética de la IA, protección frente a decisiones automatizadas y biometría. Avance hacia un Reglamento de IA complementario al RGPD.	Transición hacia modelos integrales, con influencia europea y cooperación regional (Red Iberoamericana de Protección de Datos, RIPD).	Implementación de la Ley 21.719, debates sobre datos de salud, IA y protección de menores.

Síntesis analítica

- Europa: marco más consolidado, con desarrollo doctrinal profundo y supervisión supranacional.
- América Latina: proceso de armonización y constitucionalización del derecho; fuerte influencia del RGPD.
- Chile: transición hacia un modelo europeo integral con reconocimiento constitucional explícito y ley de tercera generación (Ley 21.719).

V. Autodeterminación informativa en TEDH y Corte IDH

El presente cuadro sintetiza aquellas decisiones relevantes de la Corte Europea de Derechos Humanos (TEDH) y de la Corte Interamericana de Derechos Humanos (Corte IDH) que han configurado el estándar jurídico en materia de autodeterminación informativa y protección de datos personales.[34] Se privilegia un enfoque comparado, destacando los criterios de proporcionalidad, finalidad y salvaguardas institucionales aplicables al contexto chileno.

[34] Este cuadro se limita a decisiones de la Corte Europea de Derechos Humanos (TEDH) y de la Corte Interamericana de Derechos Humanos (Corte IDH). Si bien, el Tribunal de Justicia de la Unión Europea (TJUE) ha desarrollado jurisprudencia de influencia en materia de protección de datos personales *(Google Spain, Digital Rights Ireland, Schrems I y II)*, sus fallos pertenecen al ámbito del Derecho de la Unión Europea y no al sistema del Consejo de Europa, por lo que se excluyen de esta síntesis para preservar la coherencia institucional.

Tribunal	Caso (año)	Hechos centrales	Norma aplicable	Doctrina/estándar fijado	Utilidad práctica para la judicatura chilena
TEDH	S. and Marper v. United Kingdom (2008)	Retención indefinida de ADN y huellas de personas no condenadas.	Artículo 8 CEDH (vida privada).	La retención general e indiscriminada vulnera la proporcionalidad; exige límites temporales, finalidad específica y salvaguardas efectivas.	Referencia obligada para controles sobre conservación de datos biométricos por fuerzas de seguridad y fiscalías; impone examen de necesidad y proporcionalidad ex ante.
TEDH (Gran Sala)	Big Brother Watch and Others v. United Kingdom (2021)	Intercepción masiva de comunicaciones y cooperación internacional en inteligencia.	Arts. 8 y 10 CEDH.	La vigilancia a gran escala no es per se incompatible con la Convención, pero requiere base legal clara, control judicial previo y salvaguardas técnicas de minimización y selección.	Proporciona parámetros para autorizar o revisar medidas de vigilancia digital y retención de metadatos, exigiendo control independiente y auditoría posterior.
Corte IDH	Escher y otros v. Brasil (2009)	Intercepciones telefónicas a líderes sociales y divulgación de datos.	Artículo 11 CADH (vida privada) y garantías judiciales.	Prohíbe injerencias arbitrarias y establece criterios de legalidad, finalidad legítima, necesidad y proporcionalidad bajo control judicial efectivo.	Guía para validar interceptaciones en investigaciones penales y control judicial de medidas intrusivas de vigilancia estatal.
Corte IDH	Tristán Donoso v. Panamá (2009)	Grabación y difusión pública de conversaciones privadas de un abogado.	Arts. 11 y 13 CADH.	Vincula la privacidad con la libertad de expresión; toda divulgación estatal de datos personales requiere examen estricto de proporcionalidad y prohibición de sanciones desproporcionadas.	Criterios para ponderar la divulgación de información por autoridades públicas y los límites legítimos a la privacidad de actores públicos.
Corte IDH	Gomes Lund (*'Guerrilha do Araguaia'*) v. Brasil (2010)	Acceso a archivos estatales relativos a violaciones graves de derechos humanos.	Arts. 8, 13 y 25 CADH.	Reconoce el derecho de acceso a la información pública de víctimas y familiares; impone el deber estatal de búsqueda activa y apertura de archivos.	Establece un estándar de transparencia reforzada aplicable al acceso a expedientes y documentos con datos personales sensibles de víctimas o personas fallecidas.

Corte IDH	Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia (2023)	Durante más de dos décadas, integrantes de una organización de abogados defensores de derechos humanos fueron objeto de seguimientos, vigilancia, interceptaciones de comunicaciones, recopilación y almacenamiento de datos personales, amenazas, hostigamientos y discursos estigmatizantes por autoridades estatales, en un contexto de violencia estructural contra defensores. Las actividades incluyeron inteligencia estatal sin control efectivo, generación de archivos ilegales y falta de acceso de las víctimas a la información recopilada sobre ellas.	Convención Americana sobre Derechos Humanos: arts. 4, 5, 8, 11, 13, 16, 19, 22 y 25, en relación con el artículo 1.1. Convención de Belém do Pará (artículo 7). Principios interamericanos sobre libertad de expresión, vida privada y protección de datos personales.	La Corte consolida un estándar interamericano robusto sobre actividades de inteligencia estatal, estableciendo que: (i) toda labor de inteligencia debe cumplir reserva de ley estricta, finalidad legítima, necesidad y proporcionalidad; (ii) la recopilación, conservación y tratamiento de datos personales por órganos de inteligencia está sujeta a controles reforzados; (iii) se reconoce explícitamente el derecho a la autodeterminación informativa frente a archivos de inteligencia; (iv) se afirma el derecho a defender los derechos humanos como derecho autónomo; y (v) los discursos estigmatizantes de autoridades públicas pueden generar responsabilidad internacional por afectar honra, libertad de expresión y asociación.	Proporciona criterios directamente aplicables por tribunales chilenos para: (i) el control de legalidad y convencionalidad de actuaciones de inteligencia y contrainteligencia; (ii) la interpretación del derecho a la vida privada y a la protección de datos personales (especialmente relevante a la luz de la Ley N.º 21.719); (iii) el análisis judicial de archivos estatales y acceso a información personal; (iv) la protección reforzada de abogados, periodistas y defensores de derechos humanos; y (v) la evaluación de la responsabilidad estatal derivada de declaraciones estigmatizantes de autoridades públicas, incluso sin violencia física directa.

Capitulo 3

Marco conceptual y ámbito de aplicación de la ley

Es importante indicar que la promulgación del RGPD marcó un hito fundamental en la protección de la privacidad y de los datos personales a nivel mundial. Los datos claramente son en la actualidad un recuso muy valioso, considérese que muchos modelos de negocios a nivel mundial se basan en el uso de los datos.

La Ley 21.719 actualiza la normativa chilena respecto a la protección de la privacidad y de los datos, por lo tanto, se produce una transformación profunda. La actual ley de 1999 se denomina "Ley 19.628 sobre protección de la vida privada" y con la reforma su nombre se modificará, es decir, pasará a llamarse "Ley 19.628 sobre protección de datos personales". La doctrina chilena había criticado no en pocas ocasiones la necesidad de reformar esta ley, pues evidentemente ella no incorporaba un sinnúmero de aspectos relevantes en torno al escenario digital actual. Sin embargo, es relevante mencionar que hubo varios hitos significativos respecto a este derecho. Si bien existieron una serie de modificaciones de la Ley 19.628[35] a nivel constitucional la Ley 21.096 de 16 de junio de 2018 introdujo en el 19 Nº 4 la consagración expresa del derecho de protección de datos de la siguiente forma:

> **Artículo 19.** La Constitución asegura a todas las personas:
>
> 4º. El respeto y protección a la vida privada y a la honra de la persona y su familia, y asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley.[36]

[35] Ley 19.812 de 13 de junio de 2002; Ley 19.899 de 18 de agosto de 2003; Ley 20.463 de 20 de octubre de 2010, Ley 20.521 de 23 de julio de 2011; Ley 20575 de 17 de febrero de 2012; Ley 20.591 de 7 de junio de 2012; Ley 21.214 de 28 de febrero de 2020; Ley 21.504 de 10 de noviembre de 2022. Véase respecto de la mayoría de estos cuerpos legales el análisis de Donoso y Reusser (2021: 58-66).

[36] Contreras (2020: 87).

En cuanto al marco conceptual de la protección de datos es preciso considerar una serie de definiciones que establece la ley. Naturalmente la ley adopta un concepto amplio de datos personales y dispone:

> f) **Dato personal:** 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.
>
> Para determinar si una persona es identificable deberán considerarse todos los medios y factores objetivos que razonablemente se podrían usar para dicha identificación en el momento del tratamiento.

Es posible identificar elementos claves de esta definición. En tal sentido, el primer elemento es el relativo a la información, que comprende todo tipo o clase de información, ya sea privada, social, laboral, económica, entre otras. Contreras, Drago y Viollier clasifican esta información en objetiva y subjetiva. La primera alude a características determinadas de una persona, edad, altura, entre otras. La segunda incluye valoraciones u opiniones, por ende, se incluiría de acuerdo con los mencionados autores incluso probabilidades o predicciones referidas a una persona determinada[37].

Garrido y Saenz incluyen respecto al formato o soporte de la información tanto a los datos alfabéticos, numéricos, gráficos, fotográficos o sonoros[38].

El segundo elemento se refiere a la conexión o vínculo entre el dato y una persona concreta. Ello implica una referencia a su identidad, a sus comportamientos y por lo tanto a una serie de circunstancias que directa o indirectamente permitan efectuar esta conexión. El tercer elemento dice relación con el titular del derecho de protección de datos, esto es, una persona natural[39], lo que excluye a quienes han fallecido y a las personas jurídicas. Un cuarto elemento comprende la identificabilidad, ello es relevante pues incluye tanto la noción de persona identificada como identificable, lo que implica la aplicación de la ley al tratamiento de información que de forma aislada o asociada a otra información puede llegar a cabo con la identificación de una

[37] Contreras, Drago y Viollier (2025: 25).

[38] Garrido y Saenz (2024: 4).

[39] Artículo 55 del Código Civil. "Son personas todos los individuos de la especie humana, cualquiera que sea su edad, sexo, estirpe o condición"

persona natural. En otras palabras, las disposiciones de la ley no se aplican solo al tratamiento de datos cuando el individuo está clara y directamente identificado, sino que también es aplicable cuando existe una mera posibilidad de identificar quién es ese individuo. En Chile es habitual identificar a una persona por su cédula de identidad o su nombre, pero también otros factores son sus características físicas, genéticas, sociales. Que una persona sea identificable depende básicamente de lo fácil o difícil que sea obtener la información necesaria para identificarla[40].

Entonces, a la hora de decidir si una persona es identificable, se deben tener en cuenta todos los medios que el responsable del tratamiento u otra persona probablemente utilicen, según el criterio general, para identificar a la persona en cuestión. Por lo tanto, la mera posibilidad hipotética de identificar a una persona no es suficiente para considerarla identificable. Lo decisivo es más bien si, con un esfuerzo realista en términos de tiempo, costos y mano de obra, es posible asignar la información a una persona determinada. Por el contrario, si la identificación requiere un esfuerzo desproporcionado en los mismos términos indicados, se debe rechazar la identificabilidad, ya que el riesgo de identificación es entonces de facto insignificante. Esta temática se debatió en un asunto prejudicial respecto a un caso que se generó en Alemania: el Sr. Breyer presentó un recurso ante los tribunales contencioso-administrativos alemanes para que se prohibiera a las páginas web de los organismos federales alemanes conservar las direcciones IP de las personas que accediesen a sus sitios web. Es relevante considerar, que dichas direcciones IP eran dinámicas, por lo cual no permiten identificar, por sí mismas, a una persona natural. Con todo, la combinación con diversos datos -como por ejemplo la fecha de consulta de la web y la identificación del usuario

[40] Considerando 26 RGPD. Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable. Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos. Por lo tanto, los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación.

al acceder a la web- sí permite obtener la identidad del usuario. Es por ello que el Tribunal Supremo Alemán remitió ciertas cuestiones prejudiciales al Tribunal de Justicia Europeo, como por ejemplo, si la IP dinámica de un computador obtenida por el titular de la web puede ser considerada un dato personal, en el caso de que el proveedor de acceso a internet tenga los datos adicionales necesarios para identificar a un usuario, por ende, la duda surge en torno a si es un dato de una persona identificable, ya que podría ser considerado de forma directa o indirecta. Específicamente, en el caso de Alemania existían los medios legales para que el proveedor de servicios web obtuviese la información necesaria del proveedor de acceso a internet, así que podría disponer de medios razonables para identificar indirectamente a la persona a través de una IP dinámica. Por consiguiente, respecto de este punto el Tribunal determina que una IP dinámica constituye, respecto al titular de una web, un dato personal si dispone de medios legales para identificar al interesado con datos que obran en poder del proveedor de acceso a internet[41].

En cuanto al ámbito de aplicación material, se establece de una manera muy general y amplia, pues incluye el tratamiento de datos que se efectúe respecto de toda persona natural o jurídica, privada o pública. De esta manera, el artículo 1 inciso 2 de la ley dispone:

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

Con todo, la norma también considera excepciones. Se excluyen del ámbito de aplicación las actividades efectuadas en el ámbito de la libertad de prensa tanto a nivel constitucional como legal y las actividades que se realizan por personas naturales en un ámbito doméstico. De esta manera la norma preceptúa:

> El régimen de tratamiento y protección de datos establecido en esta ley no se aplicará 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 Política de la República. Los medios de comunicación social quedarán sujetos a las disposiciones de esta ley en lo relativo al tratamiento de datos que

[41] Sentencia del TJEU de 19.10.2016 -asunto C582-714, párrafos, 42, 44 – Breyer. El aporte fundamental de esta sentencia es la extensión del concepto de dato personal, interpretando las expresiones "identificable" e "indirectamente" para ampliar el concepto de dato personal

efectúen con una finalidad distinta a la de opinar e informar.

Tampoco serán aplicables las normas de la presente ley al tratamiento de datos que efectúen las personas naturales en relación con sus actividades personales.

Por consiguiente, en consideración al ámbito de libertad de prensa, las normas de protección de datos no son aplicables en cuanto se refieran a actividades de carácter informativas, puesto que otras operaciones o actividades que realicen los medios de comunicación que excedan el contenido del artículo 19 Nº12 de la Constitución y las leyes atingentes, especialmente la Ley 19.733 sobre Libertades de Opinión e Información y Ejercicio del Periodismo no estarán comprendidas en la excepción indicada. De esta manera, los datos personales de los trabajadores de un medio de comunicación no se incorporan a la excepción de la norma[42]. Asimismo, también quedan excluidos del ámbito de aplicación de esta ley al tratamiento de datos de personas naturales que efectúen en actividades de carácter personal, cuyo origen se puede identificar con claridad en el reglamento europeo[43] .

Respecto del ámbito de aplicación territorial, de forma similar a otras legislaciones referidas a protección de datos, la ley chilena prevé un amplio ámbito de aplicación, incluidos efectos que exceden al territorio nacional, expresado en términos amplios puede aplicarse incluso respecto de entidades o empresas que no están físicamente presentes en Chile.

En tal sentido el artículo 1° bis de la Ley de protección de datos establece que este cuerpo legal se aplica respecto del tratamiento de datos personales que se efectúe bajo cualquiera de las siguientes situaciones:

a) Cuando el responsable o mandatario estén establecidos o constituidos en el territorio nacional.

b) Cuando el mandatario, con independencia de su lugar de establecimiento o constitución, realice las operaciones de tratamiento de datos

[42] Especialmente respecto de los datos personales de los trabajadores, véase Guzmán (2025: 23-43).

[43] Considerando 18 del RGPD. El presente Reglamento no se aplica al tratamiento de datos de carácter personal por una persona física en el curso de una actividad exclusivamente personal o doméstica y, por tanto, sin conexión alguna con una actividad profesional o comercial. Entre las actividades personales o domésticas cabe incluir la correspondencia y la llevanza de un repertorio de direcciones, o la actividad en las redes sociales y la actividad en línea realizada en el contexto de las citadas actividades. No obstante, el presente Reglamento se aplica a los responsables o encargados del tratamiento que proporcionen los medios para tratar datos personales relacionados con tales actividades personales o domésticas.

personales a nombre de un responsable establecido o constituido en el territorio nacional.

c) Cuando el responsable o mandatario no se encuentren establecidos 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, independientemente de si a éstos se les requiere un pago, o a monitorear el comportamiento de titulares que se encuentran en el territorio nacional, incluyendo su análisis, rastreo, perfilamiento o predicción de comportamiento.

La presente ley también se aplicará al tratamiento de datos personales que sea realizado por un responsable al que, sin estar establecido en el territorio nacional, le resulte aplicable la legislación nacional a causa de un contrato o del derecho internacional.

Del tenor del texto legal se deduce que las hipótesis reguladas no poseen el carácter de acumulativas, por ende, pueden aplicarse de forma independiente. Otro aspecto para considerar es que el ámbito de aplicación surte efectos sin tener en cuenta la nacionalidad del titular de los datos. La primera hipótesis sigue el criterio de la territorialidad[44], pues si la empresa u organización se encuentra asentada en el territorio nacional se aplica las disposiciones chilenas. En la segunda hipótesis el criterio determinante es el responsable, pues si este está ubicado en el territorio nacional, con independencia de que el mandatario no lo esté, la ley aplicable será la ley chilena[45]. El tercer criterio considera que, aunque el procesamiento de los datos se realice fuera de Chile, pero tenga como objetivo proporcionar bienes o servicios en el territorio nacional es aplicable la ley chilena. Respecto de esta hipótesis se requiere de la designación de un representante ante la Agencia[46].

Es preciso considerar que esta norma es similar con otras legislaciones que han modernizado los estándares respecto de la protección de datos, puesto que es muy posible que el procesamiento de datos se realice en línea, por empresas extranjeras, con servidores que no se encuentran en territorio nacional. Por consiguiente, la ley establece diversos criterios vinculados con la noción de extraterritorialidad, que tienen como objetivo proteger a los titulares de los datos.

---

[44] Garrido y Sáenz utilizan la expresión del criterio del establecimiento. Garrido y Saenz (2024:8).

[45] Contreras, Drago y Viollier (2024: 23).

[46] Garrido y Sáenz (2024: 9); Pino (2025: 58).

Capitulo 4
Principios informadores y bases de legitimidad

I. Consideraciones generales. Principios: concepto y función normativa[47]

En el derecho contemporáneo, la apelación a "principios" se ha convertido en un rasgo estructural de la legislación, de la argumentación jurisdiccional y de la praxis administrativa. A pesar de que su naturaleza y función normativa está lejos de ser objeto de acuerdo, existe al menos un inventario de las alternativas que discute la teoría y maneja la praxis del derecho. Se admite que los principios operan como cláusulas de dirección del sistema normativo: condensan criterios de racionalidad jurídica, fijan parámetros de interpretación y control e irradian exigencias hacia reglas más concretas. Ocasionalmente, se incorporan a textos positivos—constituciones, leyes sectoriales, reglamentos, e incluso *soft law*— a veces con finalidad retórica, en otras con el propósito de dar coherencia a sistemas normativos crecientemente complejos; y también para permitir algún grado de disciplina jurídica de situaciones de alta variabilidad en los hechos, donde el legislador no puede (o no quiere) fijar con claridad los elementos para la construcción de la regla aplicable al caso, y traslada una parte importante de esta tarea al operador juez o funcionario administrativo.

En la teoría jurídica, la distinción entre reglas y principios ha sido elaborada desde distintas perspectivas. La tradición anglosajona, a partir de Dworkin, entiende los principios como estándares que poseen "peso" y que no operan en un esquema de todo-o-nada; pueden entrar en colisión y requieren ponderación en contextos concretos[48]. La teoría de Alexy refuerza esta idea: los principios serían "mandatos de optimización", exigencias de realización en la mayor medida posible según las posibilidades jurídicas y fácticas[49]. Sin embargo, la función normativa de los principios no se agota en la ponderación: en ámbitos regulados por autoridades administrativas

[47] Este texto se presenta de acuerdo al artículo 3° de la Ley 19.628 según modificación introducida por la Ley 21.719, artículo 1 N° 6.

[48] Dworkin (1989:72).

[49] Alexy (1983:115 y ss., 138 passim)

(como protección de datos), los principios cumplen también un rol de "programación" del ejercicio de potestades y de estructuración de deberes de diligencia, documentación y diseño organizacional.

Por ello, frente a las posibilidades enunciadas anteriormente, el operador jurídico debe asumir que la consagración expresa de principios no se agota en un posible contenido retórico, y por lo tanto debe actuar de tal modo de darle eficacia normativa.

En materia de protección de datos, los principios cumplen al menos cinco funciones:

> (1) constituyen una delimitación material del poder de tratamiento, estableciendo condiciones generales de legitimidad;
>
> (2) sirven de guía interpretativa para resolver lagunas o ambigüedades (por ejemplo, qué es un tratamiento "compatible" con la finalidad original);
>
> (3) son un elemento del estándar de diligencia y de diseño para el responsable, vinculando gobernanza interna y cumplimiento;
>
> (4) aportan un criterio de control para la autoridad, al habilitar fiscalización y sanción por infracción de deberes generales; y
>
> (5) pueden considerarse como elementos de un sistema en relación con los derechos subjetivos del titular (acceso, rectificación, supresión, oposición, portabilidad y otros) puestos que éstos podrían considerarse como la faz subjetiva de los principios de calidad, transparencia, proporcionalidad y responsabilidad, considerados éstos en una faz objetiva.

La Ley 21.719 sustituye el artículo 3° de la Ley 19.628 por uno que consagra un catálogo de principios del tratamiento, que opera como una especie de "columna vertebral" del sistema. El artículo 3° en su versión modificada, enumera los principios de: (a) licitud y lealtad; (b) finalidad; (c) proporcionalidad; (d) calidad; (e) responsabilidad; (f) seguridad; (g) transparencia e información; y (h) confidencialidad (Ley 21.719, artículo 1 N° 6).

Este acápite desarrolla el contenido de cada principio en tres planos: (i) el plano doctrinario, que recoge discusiones sobre el sentido y alcance del principio, sus tensiones internas y su lugar en la teoría general del derecho y del derecho de datos; (ii) el plano comparado, con énfasis en el Derecho de la Unión Europea (en particular RGPD), el sistema del Consejo de Europa (Convenio 108 y Protocolo de modernización "108+"), y pautas globales como las Directrices de la OCDE; y (iii) el plano sistemático-interno, que

vincula el principio con otros artículos relevantes introducidos por la Ley 21.719 (deberes del responsable: artículos 14 y ss.; bases de licitud: artículos 12 y 13; deber de secreto: artículo 14 bis; deber de transparencia: artículos 14 ter; privacidad desde el diseño: artículo 14 quáter; seguridad y reporte de brechas: artículos 14 quinquies y 14 sexies; cesión y encargo: artículos 15 y 15 bis; evaluación de impacto: artículo 15 ter; decisiones automatizadas: artículo 8° bis; y régimen sancionatorio: artículos 34 y ss.).

Desde el punto de vista del método, este capítulo combina un análisis dogmático (identificación del contenido normativo del precepto, con especial atención a su función sistemática), un análisis funcional comparado (contrastando soluciones normativas y su racionalidad) y un análisis de cumplimiento (identificando los "puntos de control" que cada principio genera en el ciclo de vida del dato).

II. Los principios en la Ley 21.719 (artículo 3° Ley 19.628 reformada)

El artículo 3° reformado establece, en forma de catálogo, los principios rectores del tratamiento de datos personales. A diferencia de otras técnicas legislativas (por ejemplo, un preámbulo o "considerandos"), aquí los principios se integran al cuerpo normativo como norma directamente aplicable, y su infracción puede derivar en responsabilidad y sanción. Su ubicación sistemática—al inicio de la ley—revela su vocación transversal: no son reglas aisladas, sino parámetros de lectura para el conjunto del régimen aplicable. La estructura del artículo 3° combina enunciados generales con reglas de cierre o concreción mínima (por ejemplo, la obligación de acreditar licitud; o la obligación de suprimir/anonimizar tras el plazo necesario).

1. Licitud y lealtad

1.1. Contenido normativo del artículo 3°

El artículo 3°, letra a), dispone que "los datos personales sólo pueden tratarse de manera lícita y leal" El principio se formula como un binomio: (i) licitud (conformidad con la ley y con las bases de legitimación) y (ii) lealtad (corrección frente al titular, evitando sorpresas, engaños o aprovechamiento indebido de asimetrías). Lo interesante de este precepto es que, en su estructura, es más que un mero principio, ya que contempla una regla que

establece un deber dirigido a garantizar su cumplimiento: "el responsable deberá ser capaz de acreditar la licitud del tratamiento de datos personales que realiza". La exigencia de "acreditar" licitud introduce un componente probatorio-organizacional cercano a la "rendición de cuentas" o *accountability:* no basta con cumplir; el responsable debe poder demostrarlo. Este deber ya contiene en sí mismo los elementos de concreción necesarios para el enunciado de una regla (lo que se aparta de la estructura de un principio).

1.2. Perspectiva doctrinal

Doctrinariamente, la licitud expresa la idea de que el tratamiento de datos no es un "hecho neutro", sino un ejercicio de poder informacional que requiere fundamento jurídico. En el modelo europeo, la licitud se conecta con la existencia de una base jurídica definida (consentimiento, contrato, obligación legal, interés público, intereses vitales, interés legítimo, etc.), pero también con el respeto de límites materiales (p. ej., categorías especiales de datos). En Chile, la ley refuerza esa estructura al mantener el consentimiento como regla general (artículo 12) y establecer otras fuentes de licitud (artículo 13), incluyendo el interés legítimo, de modo que se hace precisa una evaluación y ponderación al momento de someter a escrutinio el cumplimiento del principio[50].

La lealtad, en cambio, puede entenderse como la aplicación, al ámbito del tratamiento de datos, de la idea o noción de buena fe objetiva. El cumplimiento de este principio, aplicado a quien está habilitado para tratar datos, implica conducirse de manera que el titular pueda razonablemente anticipar, dadas las circunstancias, la información proporcionada y la relación jurídica subyacente. No es sólo una prohibición de engaño; es una exigencia de "no sorpresas" o juego limpio: el tratamiento no debe desbordar el marco de expectativas legítimas creadas por el propio responsable. En un régimen de consentimiento informado, la lealtad se vuelve condición de validez material: aun existiendo un consentimiento formal, podría discutirse la deslealtad cuando la arquitectura informativa esté diseñada para inducir decisiones contra los intereses del titular (*dark patterns*) o cuando haya aprovechamiento de vulnerabilidades cognitivas. Esta lectura se alinea con la evolución comparada, donde la "*fairness*" del RGPD se ha interpretado como una cláusula general que exige proporcionalidad y previsibilidad en el uso de datos (EDPB/WP29, 2018).

[50] Véase Contreras y Trigo (2019: 69).

La segunda frase del artículo 3(a) ("acreditar la licitud") desplaza el foco desde el titular hacia la organización. La licitud deja de ser sólo un "estado" del tratamiento para convertirse en un "deber de gobierno": el responsable debe documentar la base jurídica, la finalidad, las categorías de datos, los destinatarios, los plazos y las medidas aplicadas. En la literatura se habla de "responsabilidad proactiva" o *proactive accountability*: un modelo que reemplaza la confianza ex ante por controles de gestión y evidencia ex post[51]. En términos teóricos, esta regla es un puente entre principio (norma de dirección) y cumplimiento (sistemas internos, auditorías, matrices de riesgos).

1.3. Derecho comparado

En el RGDP, el principio equivalente se encuentra en el artículo 5(1)(a): los datos deben ser tratados "de manera lícita, leal y transparente" respecto del interesado. Esta triada integra licitud, lealtad (*fairness*) y transparencia; en Chile, en cambio, se separa la transparencia como principio autónomo (artículo 3(g)). La separación que hace la ley chilena permite, analíticamente, distinguir entre: (i) un deber de conducta "leal" en el diseño del tratamiento y (ii) un deber de información "transparente" hacia el titular. No obstante, la comparación muestra que la transparencia suele funcionar como condición práctica de la lealtad: sin información clara, la expectativa razonable del titular se distorsiona (RGDP artículo 5[52]).

En el Consejo de Europa, el Convenio 108 modernizado enfatiza el tratamiento "leal y lícito" y la exigencia de finalidades legítimas, reforzando garantías de transparencia y de control independiente (Protocolo CETS 223, 2018). Las Directrices OCDE (2013) también se basan en un núcleo de principios de legitimidad, especificación de finalidad y seguridad, incorporando además la rendición de cuentas como marco transversal (OECD, 2013). Este trasfondo comparado sugiere que Chile adopta un "mínimo global" de legitimidad, pero con una particularidad relevante: el legislador inserta explícitamente el deber de acreditar la licitud en el propio principio, anticipando una lectura sancionatoria y probatoria por parte de la Agencia.

El Derecho alemán ofrece una analogía útil: en el BDSG, para ciertos ámbitos (p. ej., tratamiento por autoridades competentes), se enumeran principios generales (*Rechtmäßigkeit; Verarbeitung nach Treu und Glauben*; *Zweckbindung*; *Datenminimierung*; *Richtigkeit; Speicherbegrenzung*;

[51] Estepa (2022:67).

[52] WP29, 2018 https://unece.org/DAM/trans/doc/2018/wp29/ECE-TRANS-WP29-2018-021e.pdf

Integrität und Vertraulichkeit), reflejando la estructura del artículo 5 RGPD (BDSG, § 47). La inclusión de "*Treu und Glauben*" es especialmente cercana a la "lealtad" chilena y puede leerse como una exigencia de corrección material en la relación responsable–titular, más allá del mero cumplimiento formal.

1.4. Relaciones sistemáticas dentro de la Ley 21.719

La licitud se articula con las bases de legitimación de los artículos 12 y 13. El consentimiento es regla general (artículos 12), y debe ser libre, informado y específico. Las "otras fuentes" (artículo 13) permiten tratamiento sin consentimiento en hipótesis tipificadas; dentro de ellas, destaca la figura del interés legítimo (artículo13, letra d)), que requiere ponderar derechos y libertades del titular y puede activar el derecho de oposición previsto en el artículo 8, letra a). Esta arquitectura refuerza la licitud como concepto relacional: depende de la finalidad, del contexto y de la medida en que el responsable pueda justificar el tratamiento de datos.

El deber de "acreditar licitud" se conecta explícitamente con obligaciones del artículo 14: el responsable debe informar y poner a disposición del titular antecedentes que acrediten licitud, así como entregar información relevante sobre el tratamiento. La licitud se vuelve así un deber de "auditabilidad" y "explicabilidad" jurídica. En litigios o procedimientos administrativos, la carga argumental recae en el responsable, lo que es coherente con un modelo de asimetrías informativas.

La lealtad, por su parte, se vincula con el principio de finalidad (artículo 3(b)) y con las reglas de compatibilidad o cambio de finalidad. Un tratamiento "sorpresivo" será, *prima facie*, desleal. También se relaciona con la regulación de decisiones automatizadas (artículo 8° bis) y con la evaluación de impacto (artículo 15 ter), pues tratamientos de alto riesgo exigen medidas de mitigación y, en su caso, consulta a la Agencia. Un responsable que omite evaluar impactos en tratamientos intensivos puede considerarse desleal en términos institucionales.

Finalmente, en el plano sancionatorio, la infracción de deberes de información (artículo14 ter), de secreto (artículo14 bis) o de seguridad (artículo14 quinquies) suele implicar, además, un déficit de licitud o lealtad. En este sentido, la letra a) opera como una especie de "techo" o cobertura general que permite articular infracciones materiales y organizacionales en un mismo reproche, especialmente cuando el tratamiento carece de base jurídica o excede lo razonablemente esperable.

2. Confidencialidad

2.1. Contenido normativo del artículo 3°

El artículo 3°, letra h), dispone que "el responsable de datos personales y quienes tengan acceso a ellos deberán guardar secreto o confidencialidad" y que el responsable "establecerá controles y medidas adecuadas para preservar el secreto o confidencialidad", precisando que el deber subsiste aun después de concluida la relación con el titular. Del mismo modo que en el caso anterior, aquí el principio va asociado un deber general de reserva, de naturaleza organizacional (deber de adoptar controles internos) y personal (deberes u obligaciones de quienes acceden a los datos), con un efecto temporal extendido.

2.2. Perspectiva doctrinal

La confidencialidad constituye un principio clásico del derecho de datos y, al mismo tiempo, un puente con ámbitos profesionales históricamente vinculados al secreto (medicina, banca, abogacía). En protección de datos, no se identifica con "secreto profesional" en sentido estricto, sino con un deber de impedir accesos, usos o divulgaciones no autorizadas, incluso dentro de la propia organización. Doctrinariamente, se ha subrayado que la confidencialidad no es sólo un interés del titular, sino un presupuesto de confianza en entornos digitales y, por tanto, un componente de legitimidad del ecosistema informacional[53].

La cláusula de subsistencia del deber después del término de la relación con el titular introduce una dimensión relevante: la temporalidad del vínculo jurídico no agota la obligación. Este rasgo aproxima el principio a la lógica fiduciaria: quien accede a datos en virtud de una relación (laboral, contractual, estatutaria) asume un deber de reserva que no decae por el solo término del vínculo. Ello se justifica por la permanencia del riesgo: la revelación posterior puede ser tan lesiva como la contemporánea, y el titular no controla la circulación futura de su información.

En términos de cumplimiento, la confidencialidad exige gobernanza de accesos *(need-to-know)*, segregación de funciones, registros de acceso, cláusulas contractuales de confidencialidad, formación, y sanciones internas. El principio también tiene una dimensión interpretativa: ante ambigüedad, la regla debiera inclinarse por el tratamiento más restrictivo en cuanto a

[53] OECD (2013).

divulgación, especialmente tratándose de datos sensibles o especialmente protegidos. Asimismo, la confidencialidad interactúa con la transparencia: informar no significa divulgar datos a terceros; y facilitar el ejercicio de derechos no autoriza accesos indiscriminados. El principio ordena modular flujos de información según rol, finalidad y base jurídica.

Por otro lado, se ha planteado que este principio (o principio/deber) como deber de diligencia y cuidado, al extenderse más allá de un deber de no divulgación hacia un área de protección del secreto, conlleva también la necesidad del agente de realizar una adecuada evaluación de riesgos de tal modo de poder demostrar que el nivel de seguridad adoptado es adecuado a los riesgos previsibles[54]. Esto vincula el principio de confidencialidad con el de seguridad que se trata más adelante.

2.3. Derecho comparado

En el RGPD, la confidencialidad aparece integrada en el principio de "integridad y confidencialidad" (artículo 5(1)(f)), que exige un tratamiento que garantice seguridad adecuada, incluida la protección contra tratamiento no autorizado o ilícito y contra pérdida o daño. Chile separa seguridad (artículo 3(f)) de confidencialidad (artículo 3(h)), lo que permite distinguir la seguridad alusiva a un conjunto de medidas (técnicas y organizativas) frente a amenazas; la confidencialidad define, más bien, un deber de reserva y control sobre la comunicación y el acceso. Esta separación puede ser útil para el razonamiento sancionatorio: puede haber violación de confidencialidad sin "incidente de seguridad" (p. ej., divulgación voluntaria por un empleado).

El Derecho francés, a través de la CNIL, enfatiza que la seguridad incluye confidencialidad, integridad y disponibilidad, y que la obligación de seguridad debe ser proporcional al riesgo[55]. En Italia, el *Garante per la protezione dei dati personali* explica los "*principi fondamentali*" del artículo 5 RGPD como base del sistema, destacando la *riservatezza/integritá* junto con la *accountability*[56]. Este trasfondo muestra que la confidencialidad es un componente común, aunque se formule como parte de seguridad o como deber autónomo.

En instrumentos globales, la confidencialidad se suele expresar como "*security safeguards*" (OCDE) o como deber de impedir divulgación no autorizada (Convenio 108). La modernización del Convenio 108 refuerza

[54] Contreras, Drago y Viollier (2024: 58).

[55] CNIL, "RGPD—Chapitre II" (2018); service-public.fr (2024).

[56] Sitio oficial del Garante, https://www.gpdp.it/regolamentoue, consultado el 22.1.2026.

obligaciones de seguridad y responsabilidad, pero también el papel de autoridades independientes y remedios efectivos, lo que incrementa el valor práctico de la confidencialidad como estándar justiciable[57].

2.4. Relaciones sistemáticas dentro de la Ley 21.719

La Ley 21.719 desarrolla la confidencialidad en disposiciones específicas: el artículo 14 bis regula el "deber de secreto o confidencialidad" del responsable, reiterando la subsistencia posterior al término de la relación y estableciendo reglas para datos provenientes de fuentes de acceso público cuando el responsable los organiza, clasifica o combina (artículo 14 bis). Esta norma permite concretar cuándo el responsable debe "reconstituir" el secreto al crear valor agregado sobre datos que eran públicamente accesibles.

La confidencialidad se vincula además con el régimen de encargo o tratamiento por tercero mandatario (artículo15 bis), pues el encargado debe cumplir deberes de secreto y seguridad, y tiene prohibición de tratar para objeto distinto o ceder sin autorización. La regla de devolución o supresión al término del encargo es también una concreción de confidencialidad y finalidad.

El principio se proyecta sobre el régimen sancionatorio: el texto legal tipifica infracciones vinculadas a vulnerar el deber de secreto o confidencialidad (v.gr., referencias a infracciones en torno al artículo 14 bis). En consecuencia, la confidencialidad opera como estándar primario de reproche y como criterio agravante cuando su infracción se combina con otros déficits (p. ej., falta de medidas de seguridad).

Finalmente, la confidencialidad debe ser leída en conjunto con transparencia (artículo 3 g) y artículo14 ter): la obligación de informar al titular no habilita la divulgación a terceros ni la exposición de datos en procesos de atención. Un diseño adecuado debe permitir entregar información y facilitar derechos sin comprometer confidencialidad, por ejemplo, mediante autenticación robusta y procedimientos de verificación de identidad.

[57] CETS 223 (2018).

3. Transparencia e información

3.1. Contenido normativo del artículo 3°

El artículo 3°, letra g), establece que el responsable debe entregar al titular "toda la información que sea necesaria para el ejercicio de los derechos" reconocidos por la ley, "incluyendo las políticas y las prácticas" sobre tratamiento, las cuales deben estar "permanentemente accesibles" de manera "precisa, clara, inequívoca y gratuita". Agrega un deber de facilitación: el de adoptar medidas adecuadas y oportunas para facilitar el acceso a la información y las comunicaciones relativas al tratamiento. Se trata de un principio que combina: (i) contenido informativo mínimo (políticas/prácticas), (ii) cualidades del lenguaje (claridad, inequívoco) y (iii) condiciones de acceso (permanencia y gratuidad).

3.2. Perspectiva doctrinal

La transparencia es, en el derecho de datos, un presupuesto de autonomía informativa. Sin información suficiente y comprensible, el titular no puede evaluar riesgos, ejercer derechos ni oponerse a usos no deseados. A diferencia de la publicidad administrativa clásica (que busca controlar al poder público), aquí la transparencia tiene un sentido relacional: reduce asimetrías entre responsable y titular, particularmente en mercados digitales donde el tratamiento es opaco y automatizado. La transparencia se asocia además con la "explicabilidad" y con la calidad de la comunicación: no basta con proveer información; debe ser utilizable por el destinatario promedio[58].

Doctrinalmente, se distinguen dos capas: transparencia ex ante y ex post. La primera opera al momento de la recolección (informar finalidades, bases jurídicas, destinatarios, plazos, transferencias, derechos, etc.). La segunda opera durante el ciclo de vida del dato: comunicaciones sobre cambios de finalidad, brechas de seguridad, cesiones, decisiones automatizadas, y respuesta a solicitudes de ejercicio de derechos. La Ley 21.719 adopta esta lógica al vincular transparencia con el "ejercicio de derechos", no sólo con el acto inicial de recolección.

Un punto crítico es la tensión entre transparencia y sobrecarga informativa. La doctrina ha advertido que "más información" puede equivaler a "menos comprensión" cuando se ofrece en formatos extensos o técnicos. La exigencia legal de precisión, claridad y de lenguaje inequívoco introduce, por tanto, un criterio de calidad normativa de la información: debe ser relevante,

[58] WP29/EDPB, 2018

ordenada, y redactada en un lenguaje comprensible. Esto conecta con la idea de "transparencia material", distinta de la transparencia meramente formal (cumplimiento por *checklists*).

En el plano del diseño regulatorio, la transparencia funciona como vector de prevención de prácticas desleales. Si el responsable debe exponer políticas y prácticas de manera accesible, se dificulta el uso de técnicas encubiertas de extracción de datos. En este sentido, transparencia e información son condición de lealtad, pero también de proporcionalidad: cuando el responsable explica el porqué y el para qué, se vuelve más escrutable la necesidad del dato. La evaluación de impacto (artículo 15 ter) también presupone transparencia interna (documentación) y, en ciertos casos, transparencia hacia el titular o hacia la Agencia.

3.3. Derecho comparado

El RGDP integra transparencia en el principio general del artículo 5(1)(a) y desarrolla deberes de información en los artículos 12 a 14 (información, comunicación y modalidades). Las "*Guidelines on Transparency*" del antiguo Grupo de Trabajo del artículo 29[59], hoy asumidas por el EDPB, enfatizan que la transparencia se concreta en: (1) información al interesado; (2) comunicaciones sobre derechos; y (3) facilitación del ejercicio de derechos, con lenguaje claro y accesible. El diseño chileno converge al exigir claridad y facilitar el acceso, aunque con fórmulas propias (por ejemplo, gratuidad como regla expresa en el artículo 3(g)).

En Francia, la CNIL sistematiza los principios del Capítulo II del RGPDr, destacando transparencia como elemento esencial de *licéité/loyauté* y como base para el control de los interesados[60]. En Alemania y Austria, la doctrina y guías de autoridades subrayan que transparencia exige que las comunicaciones sean "*leicht zugänglich und verständlich*" (fácilmente accesibles y comprensibles), coherente con la exigencia chilena de claridad y lenguaje inequívoco[61].

En la OCDE, la transparencia se expresa en el principio de "*Openness*" (apertura): se requiere una política general de apertura sobre desarrollos, prácticas y políticas respecto de datos personales, y medios fácilmente disponibles para establecer la existencia y naturaleza de los datos, su finalidad

[59] WP260 rev.01 (2018).

[60] CNIL (2018).

[61] WKO (2024).

y la identidad del responsable[62]. Chile adopta una lógica similar al exigir políticas y prácticas permanentemente accesibles.

Un contraste relevante: en el RGPD existe un régimen de costos en ciertas respuestas (p. ej., solicitudes manifiestamente infundadas o excesivas), pero la regla general es gratuidad y facilidad. Chile enfatiza expresamente la gratuidad en el principio, lo que sugiere una lectura pro-titular. Esta opción legislativa puede ser especialmente relevante en contextos de asimetría socioeconómica, donde el costo de acceso a información o derechos podría tener efectos excluyentes.

3.4. Relaciones sistemáticas dentro de la Ley 21.719

El principio se desarrolla en el artículo 14 ter ("deber de información y transparencia"), que obliga al responsable a mantener a disposición del público, en su sitio web u otro medio equivalente, información mínima, incluyendo la política de tratamiento, su fecha y versión, y otros elementos. De esta forma, el principio del artículo 3(g) se operacionaliza mediante un *checklist* legal de transparencia permanente.

Se conecta estrechamente con los derechos del titular del Título I (artículos 4 y ss.), especialmente el derecho de acceso (artículo 5), que incluye información sobre finalidad, destinatarios, período de tratamiento e intereses legítimos cuando aplique. La transparencia es, por tanto, tanto un deber general como un contenido específico del derecho de acceso.

El deber de transparencia también es crucial en decisiones automatizadas (artículo 8° bis). El derecho de acceso incluye "información significativa sobre la lógica aplicada" cuando el tratamiento se realice conforme a ese precepto, lo que introduce una exigencia de explicabilidad mínima, especialmente relevante en sistemas de *scoring* y perfiles[63].

Finalmente, transparencia se relaciona con la responsabilidad y con la acreditación de licitud: el responsable debe poder mostrar antecedentes de licitud (artículo14) y, al mismo tiempo, comunicar al titular información necesaria. En caso de brechas de seguridad, los deberes de reporte (artículo 14 sexies) presuponen mecanismos comunicacionales claros y oportunos; una organización sin canales de transparencia efectiva verá comprometida su capacidad de cumplir los deberes de notificación y, en consecuencia, su responsabilidad administrativa.

[62] OECD (2013).

[63] Véase Campos (2024:11)

4. Seguridad

4.1. Contenido normativo del artículo 3°

El artículo 3°, letra f), prescribe que el responsable debe "garantizar estándares adecuados de seguridad", protegiendo los datos contra "tratamiento no autorizado o ilícito" y contra "pérdida, filtración, daño accidental o destrucción", añadiendo que las medidas deben ser "apropiadas y acordes" con el tratamiento y la naturaleza de los datos. La norma adopta un enfoque de adecuación: no impone un catálogo fijo de medidas, sino un estándar relativo (adecuado/apropiado), dependiente de riesgo, contexto y tipo de dato.

4.2. Perspectiva doctrinal

La seguridad en protección de datos se comprende hoy como un deber de gestión de riesgos (*risk management*) más que como un conjunto estático de controles técnicos. La doctrina comparada ha desplazado el enfoque desde "seguridad informática" hacia "seguridad del tratamiento", incorporando dimensiones organizativas: políticas, procedimientos, capacitación, gestión de incidentes, continuidad operacional, y gobernanza de proveedores. Ello se debe a que las brechas no provienen sólo de fallas técnicas; también emergen de errores humanos, configuraciones inadecuadas, contratos débiles y ausencia de cultura de cumplimiento.

El principio chileno explicita un catálogo de amenazas (no autorizado o ilícito; pérdida; filtración; daño; destrucción), que puede leerse como un mapa de objetivos de seguridad: confidencialidad (evitar accesos/divulgación no autorizados), integridad (evitar alteración o daño), y disponibilidad/continuidad (evitar pérdida o destrucción). Aunque "disponibilidad" no se nombra, está implícita en la categoría "pérdida y destrucción", especialmente en sistemas críticos (salud, banca).

El criterio de adecuación ("apropiadas y acordes") requiere un juicio de proporcionalidad técnica: la medida debe ser idónea para reducir riesgos relevantes, y su intensidad debe correlacionarse con la probabilidad y gravedad del daño. La literatura reciente ha problematizado la noción de "riesgo" en DPIAs, mostrando que su definición suele ser ambigua y que las evaluaciones pueden convertirse en rituales si no se precisa qué se entiende por riesgo para derechos y libertades. Esto es particularmente pertinente porque la Ley 21.719 incorpora explícitamente un enfoque de riesgo tanto en seguridad (artículos 14 quinquies) como en evaluación de impacto (artículo 15 ter).

Seguridad, en suma, no es un "principio técnico" desconectado de derechos: su finalidad es proteger a las personas contra daños materiales e inmateriales derivados de tratamientos no controlados (fraude, discriminación, pérdida de oportunidades, afectación reputacional, vigilancia indebida). Por ello, la seguridad debe interpretarse sistemáticamente en conexión con la licitud, la lealtad y la proporcionalidad: medidas robustas pueden ser requeridas no sólo por el tipo de dato, sino también por el tipo de decisión que se adopta en base a esos datos (p. ej., *scoring* crediticio).

4.3. Derecho comparado

El RGPD recoge seguridad como parte del principio de integridad y confidencialidad (artículo 5(1)(f)) y la desarrolla en el artículo 32 (seguridad del tratamiento), con un enfoque explícito de "riesgo" y de medidas técnicas y organizativas apropiadas. Chile adopta un lenguaje muy cercano ("estándares adecuados", "medidas apropiadas", "naturaleza de los datos") y refuerza el componente probatorio al establecer, en el artículo 14 quinquies, que las medidas deben considerar estado de la técnica, costos, naturaleza/alcance/contexto/fines y la probabilidad y gravedad de riesgos. Esta convergencia sugiere una voluntad de alineamiento con el estándar europeo.

La práctica comparada de autoridades como la CNIL en Francia o guías estatales suele traducir este estándar en familias de controles (control de acceso, cifrado, respaldo, registro, segregación, pruebas, respuesta a incidentes). El derecho francés para empresas enfatiza expresamente "*garantir un niveau de sécurité adapté au risque*" y recomienda inventariar tratamientos y evaluar riesgos (service-public.fr, 2024), lo que coincide con la lógica chilena de DPIA y con el deber de reportar vulneraciones.

En instrumentos globales, la OCDE formula un principio de "*Security Safeguards*" que exige salvaguardas razonables contra riesgos como pérdida o acceso no autorizado, destrucción, uso, modificación o divulgación[64]. El Convenio 108 también contiene obligaciones de seguridad y establece que los datos deben tratarse de manera que se garantice un nivel adecuado de protección. Estas referencias comparadas corroboran que la formulación chilena se inserta en una tradición consolidada, aunque su eficacia dependerá de la densificación por instrucciones generales de la Agencia y por estándares sectoriales.

[64] OECD (2013).

4.4. Relaciones sistemáticas dentro de la Ley 21.719

La seguridad se operacionaliza en el artículo 14 quinquies ("deber de adoptar medidas de seguridad"), que obliga a adoptar medidas necesarias para resguardar el cumplimiento del principio de seguridad, considerando estado de la técnica, costos, naturaleza/alcance/contexto/fines, probabilidad de riesgos y gravedad de efectos. El mismo precepto dispone que, en sede judicial o administrativa, corresponderá al responsable acreditar la existencia y funcionamiento de medidas de seguridad adoptadas en base a niveles de riesgo y tecnología disponible. Este elemento probatorio refuerza el puente entre seguridad y responsabilidad.

El artículo 14 sexies impone un deber de reportar vulneraciones a medidas de seguridad a la Agencia, sin dilaciones indebidas, por medios expeditos. Esto crea un "ciclo de incidentes" que incluye detección, evaluación, contención, notificación y mejora. La seguridad deja de ser estática y se vuelve dinámica: aprender de incidentes forma parte del cumplimiento.

La evaluación de impacto (artículo. 15 ter) también se conecta con seguridad: exige evaluar riesgos y medidas de mitigación antes de iniciar tratamientos de alto riesgo. De este modo, la seguridad se integra al diseño, no sólo a la operación, reforzando la lógica de "*privacy by design*" del artículo14 quáter.

Finalmente, la seguridad articula con confidencialidad (artículo 3(h) y artículos. 14 bis) y con el régimen sancionatorio, que tipifica infracciones por vulnerar obligaciones de seguridad. En un enfoque sistemático, la seguridad es un principio que atraviesa todo el estatuto: sin seguridad, la licitud y la transparencia se vuelven ilusorias, pues el titular no controla quién accede y para qué se usa su información.

5. Finalidad

5.1. Contenido normativo del artículo 3°

El artículo 3°, letra b), exige que los datos sean recolectados con fines "específicos, explícitos y lícitos", y que el tratamiento se limite al cumplimiento de esos fines. Además, formula una prohibición y excepciones: no se pueden tratar datos con fines distintos a los informados al momento de la recolección, salvo que (i) el nuevo fin sea compatible con los autorizados originalmente; (ii) exista relación contractual o precontractual que justifique un fin distinto, enmarcado en fines del contrato o coherente con tratativas; (iii) el titular otorgue nuevamente su consentimiento; o (iv) lo disponga la

ley. Es uno de los principios más densificados del artículo 3°, pues incluye un régimen de cambio o ampliación de finalidad.

5.2. Perspectiva doctrinal

La finalidad (*purpose limitation*) constituye el núcleo de la protección de datos desde el paradigma de las "*Fair Information Practices*". Su racionalidad es doble: (1) evita la acumulación de poder informacional mediante usos secundarios imprevisibles (*function creep*); y (2) permite evaluar licitud y proporcionalidad en relación con objetivos concretos. Sin finalidad determinada, no hay criterio para medir necesidad, pertinencia ni plazo de conservación. En consecuencia, la finalidad es condición de inteligibilidad del tratamiento.

El legislador chileno exige que los fines sean específicos y explícitos. "Específico" apunta a un grado de determinación suficiente para permitir control; "explícito" exige que esté formulado de manera expresa y comunicada, lo que conecta con transparencia. Además, la finalidad debe ser lícita: no puede perseguir objetivos prohibidos por el ordenamiento (p. ej., discriminación ilícita) ni contrarios a derechos fundamentales.

El tratamiento para fines distintos a los informados es, por regla general, prohibido. La ley reconoce, sin embargo, hipótesis típicas de "reconducción": (i) compatibilidad; (ii) relación contractual/precontractual; (iii) nuevo consentimiento; (iv) ley. Doctrinalmente, la compatibilidad es la noción más compleja: requiere un juicio contextual sobre cercanía entre finalidades, expectativas razonables, naturaleza del dato, impacto sobre el titular y garantías adicionales. En el ámbito europeo, este test se encuentra densificado por el artículo 6(4) RGPD; Chile no lo reproduce literalmente, pero su cláusula de compatibilidad sugiere que la Agencia deberá elaborar criterios mediante instrucciones generales o decisiones caso a caso.

En la economía digital, la finalidad enfrenta retos por el uso intensivo de analítica, IA y perfiles. El "uso secundario" de datos (*secondary use*) es tema central en debates sobre *credit scoring*, publicidad conductual y sistemas de recomendación. Estudios sobre *scoring* crediticio muestran cómo la finalidad original de evaluar solvencia puede condicionar o restringir usos posteriores (p. ej., entrenar modelos) y cómo la minimización y el plazo de conservación se vuelven dependientes del propósito[65]. Por ello, el principio de finalidad debe ser aplicado con sensibilidad tecnológica: no basta enunciar

[65] Campos (2024:111).

un fin amplio ("mejorar servicios"); se requiere especificación punto a punto cuando el riesgo para el titular es alto.

5.3. Derecho comparado

El RGPD formula el principio de finalidad en el artículo 5(1)(b): los datos deben ser recogidos con fines determinados, explícitos y legítimos, y no tratados ulteriormente de manera incompatible; el tratamiento ulterior con fines de archivo en interés público, investigación científica/histórica o estadísticos no se considera incompatible bajo ciertas garantías. El artículo 6(4) ofrece criterios para evaluar compatibilidad. El legislador chileno adoptó una estructura semejante, aunque optando por listar excepciones distintas: incluye expresamente relación contractual o precontractual, el nuevo consentimiento, y remite a la ley como habilitación.

Las Directrices OCDE incorporan un principio de "*Purpose Specification*" y, separado, un principio de "*Use Limitation*", con excepciones por consentimiento o autoridad legal[66]. Este paralelismo es notable: la letra b) chilena combina ambos componentes en una misma disposición. En instrumentos interamericanos, los principios de la OEA/CJI también parten por finalidades legítimas y lealtad, enfatizando determinación del propósito y limitación de uso[67].

En derecho italiano y francés, el principio se comprende como límite central al "*riuso*" de datos, especialmente en contextos de *big data*. La doctrina europea discute el riesgo de que finalidades amplias o ambiguas vacíen el principio. Por ello, autoridades de protección de datos suelen exigir que finalidades sean "*specific and clear*" y que cambios relevantes impliquen nueva base jurídica o información adicional. La comparación sugiere que la eficacia del principio chileno dependerá de cómo se interprete "compatible" y de cuán exigente sea el estándar de especificidad.

5.4. Relaciones sistemáticas dentro de la Ley 21.719

El principio de finalidad se conecta con el derecho de acceso (artículo 5), que exige informar la finalidad o finalidades del tratamiento; también con el deber de información y transparencia (artículo 14 ter), que exige política

[66] OECD (2013).

[67] OEA/CIJ (2021).

de tratamiento y elementos esenciales del procesamiento. Si la finalidad se modifica, la transparencia exige comunicación actualizada.

En el régimen de cesión (artículo. 15), la finalidad funciona como límite: los datos pueden cederse con consentimiento y para el cumplimiento de fines del tratamiento. Además, la cesión puede ser necesaria para ejecución contractual o por interés legítimo, entre otras hipótesis. Así, el principio de finalidad opera como restricción de flujos a terceros: la cesión fuera de finalidad tiende a ser ilícita y desleal.

La finalidad también incide en proporcionalidad (minimización y conservación) y en la evaluación de impacto (artículo 15 ter), que exige describir operaciones, finalidad, evaluar necesidad y proporcionalidad, y riesgos. Por ello, la finalidad es el punto de partida metodológico de toda DPIA. En decisiones automatizadas y perfiles (artículo 8° bis), la finalidad de automatizar y su impacto sobre el titular deben ser comunicados y justificados, y pueden activar oposición. La finalidad es, en suma, el eje que articula licitud (base jurídica), transparencia (información) y control (derechos).

6. Proporcionalidad

6.1. Contenido normativo del artículo 3°

El artículo 3°, letra c), establece que los datos tratados deben limitarse "estrictamente" a los que sean "necesarios, adecuados y pertinentes" en relación con los fines. Agrega una regla temporal: los datos pueden conservarse sólo por el período necesario para cumplir fines; luego deben ser suprimidos o anonimizados, sin perjuicio de excepciones legales. Un plazo mayor requiere autorización legal o consentimiento del titular. La norma integra, en una misma letra, dos subprincipios: minimización (en volumen y tipo de dato) y limitación de conservación (*storage limitation*).

6.2. Perspectiva doctrinal

La proporcionalidad, en protección de datos, no coincide exactamente con la proporcionalidad constitucional clásica (examen de la idoneidad, necesidad, y proporcionalidad en sentido estricto). Sin embargo, comparte su racionalidad: controlar el exceso de intervención. En datos, el exceso puede darse en tres dimensiones: (i) exceso en recolección (se recogen datos no necesarios), (ii) exceso en uso (se usan datos para fines marginales o

secundarios), y (iii) exceso en conservación (se retienen más tiempo del necesario). El artículo 3(c) aborda (i) y (iii) directamente, y se conecta con (ii) a través de finalidad y licitud.

El estándar "estrictamente necesario" sugiere una lectura exigente: el responsable debe justificar por qué cada categoría de dato contribuye de modo necesario o al menos pertinente a la finalidad. Esto exige una cultura de diseño de formularios y procesos basada en "*need-to-have*" en vez de "*nice-to-have*". En práctica, la proporcionalidad se operacionaliza mediante inventarios de datos, matrices de mapeo (dato–finalidad–base jurídica), y eliminación de campos superfluos.

La regla de conservación (suprimir o anonimizar) introduce un deber de ciclo de vida. Suprimir es eliminar de modo irreversible o poner fuera de uso; anonimizar es romper el nexo con el titular, de manera que el dato deje de ser personal. La elección entre supresión y anonimización tiene implicancias: la anonimización permite usos estadísticos o de investigación, pero requiere estándares robustos para evitar reidentificación. Además, la regla "sin perjuicio de excepciones legales" reconoce que ciertos sectores requieren retención (p. ej., obligaciones tributarias, laborales, sanitarias), pero exige base legal o consentimiento para ampliar plazos.

La doctrina ha señalado que la retención excesiva es una fuente principal de daños: a mayor tiempo, mayor probabilidad de brechas o usos secundarios. Por ello, la proporcionalidad temporal es también una medida de seguridad. En sistemas de *scoring* o perfiles, el debate sobre cuánto tiempo conservar datos (historial crediticio, comportamiento digital) está intensamente vinculado a justicia y no discriminación, pues datos antiguos pueden perpetuar estigmas[68].

6.3. Derecho comparado

En el RGDP, la minimización es un principio autónomo (artículo 5(1)(c)) y la limitación del plazo de conservación es otro (artículo. 5(1)(e)). Por su parte, Chile los reúne bajo "proporcionalidad", lo que tiene ventajas e inconvenientes. La principal ventaja es que permite un razonamiento unitario sobre el exceso material y temporal del tratamiento. El inconveniente es que puede difuminar la autonomía conceptual de cada subprincipio. Con todo, la redacción chilena es sustantivamente equivalente al estándar europeo: "adecuados, pertinentes y limitados a lo necesario", y de conservación sólo por el tiempo necesario.

[68] Campos (2024:111).

Las Directrices OCDE incluyen "*Collection Limitation*", "*Data Quality*" y "*Use Limitation*", pero también consideran que las medidas deben ser proporcionales al contexto. En el sistema interamericano, los principios de la OEA/CJI también incluyen proporcionalidad y pertinencia, subrayando que la recolección debe limitarse a lo necesario para finalidades legítimas[69].

En Alemania, el artículo 5 GDPR es a menudo presentado como "*Datenminimierung*" y "*Speicherbegrenzung*"; guías de autoridades y cámaras de comercio explican que estos principios son fundamentales y se conectan con documentación y *accountability*[70]. La comparación sugiere que Chile, al incorporar la regla de supresión/anonimización, apunta a una lectura robusta de *storage limitation*, lo que puede tener efectos importantes en litigios sobre retención indefinida de bases de datos.

6.4. Relaciones sistemáticas dentro de la Ley 21.719

La proporcionalidad se conecta con el derecho de supresión (artículo 7), que permite eliminar datos cuando no resulten necesarios para la finalidad, cuando sean ilícitos o caducos, etc. En efecto, el artículo 7(a) ("datos no necesarios") es una concreción directa de la proporcionalidad. Asimismo, el derecho de oposición (artículo 8) puede operar cuando el tratamiento se base en interés legítimo y el responsable no logre acreditar motivos imperiosos, lo que implica un juicio de proporcionalidad entre intereses.

El deber de protección desde el diseño y por defecto (artículo 14 quáter) exige aplicar medidas técnicas y organizativas adecuadas considerando estado de la técnica, costos, naturaleza/ámbito/contexto/fines y riesgos, con el propósito de cumplir principios y derechos. La proporcionalidad es central "por defecto": la configuración estándar debe minimizar datos y retener por plazos limitados, salvo elección informada del titular o exigencia legal.

La evaluación de impacto (artículo 15 ter) exige evaluar necesidad y proporcionalidad respecto de la finalidad, además de riesgos y mitigaciones. Así, el principio de proporcionalidad es un criterio explícito del instrumento preventivo más importante del nuevo régimen.

La proporcionalidad también se proyecta sobre transferencias internacionales (Título V, artículos 27 y ss.) en la medida que los flujos transfronterizos deben limitarse a lo necesario para la operación y bajo garantías que den cuenta de los principios de esta ley. Aunque la relación es indirecta, la idea de

[69] OEA/CJI (2021).

[70] IHK Rhein-Neckar (2025).

"limitación" de flujos es un modo de proporcionalidad espacial. Por último, el régimen sancionatorio puede utilizar la proporcionalidad como criterio de gravedad: recolección masiva o conservación indefinida tienden a aumentar el daño potencial y justificar sanciones más severas.

7. Calidad

7.1. Contenido normativo del artículo 3°

El artículo 3°, letra d), establece que los datos deben ser "exactos, completos, actuales y pertinentes" en relación con su proveniencia y los fines del tratamiento. La norma define una exigencia de calidad informacional que combina atributos de veracidad (exactitud), integridad (completitud), actualización (actualidad) y pertinencia contextual (relevancia respecto de origen y finalidad).

7.2. Perspectiva doctrinal

La calidad es un principio con fuerte dimensión epistémica: el derecho de datos presupone que decisiones basadas en información errónea o desactualizada generan injusticias. La protección de datos no es sólo protección de intimidad; también es protección contra el poder de clasificación y evaluación injustificada. En contextos de perfiles, *scoring* y decisiones automatizadas, la calidad de datos es determinante, porque errores se amplifican por automatización y pueden afectar oportunidades de crédito, empleo o servicios.

Doctrinariamente, la calidad incluye deberes activos y reactivos. Deberes activos: diseñar procesos para captar datos correctos, validarlos, y actualizar cuando sea razonable. Deberes reactivos: corregir cuando el titular solicita rectificación y cuando el responsable toma conocimiento de inexactitud. La ley chilena refuerza el componente reactivo a través del derecho de rectificación (artículo 6) y del deber de comunicar rectificaciones a destinatarios, salvo imposibilidad o esfuerzo desproporcionado.

La referencia a la "proveniencia" sugiere que la calidad no se mide sólo por el estado del dato, sino por su origen y trazabilidad: fuentes de acceso público, datos entregados por el titular, datos inferidos o derivados, y datos obtenidos de terceros tienen niveles de confiabilidad y deberes de verificación distintos. En *scoring* crediticio, por ejemplo, se discute la calidad de datos derivados de comportamiento digital o de *proxies* socioeconómicos, que pueden ser inexactos o discriminatorios por correlaciones espurias. Así,

la calidad debe leerse también con un lente de justicia algorítmica: datos "exactos" pueden aun así ser inapropiados si capturan sesgos estructurales.

La pertinencia respecto de fines conecta calidad con proporcionalidad y finalidad: un dato puede ser exacto pero irrelevante; su tratamiento sería desproporcionado. Por ello, calidad no se reduce a exactitud, sino a idoneidad del dato para el propósito. La doctrina comparada suele integrar esta idea bajo "*data minimisation*" y "*accuracy*", pero el texto chileno explicita la pertinencia como parte de calidad, mostrando una comprensión holística.

7.3. Derecho comparado

El RGPD consagra exactitud en el artículo 5(1)(d): los datos deben ser exactos y, cuando sea necesario, estar actualizados; se deben adoptar medidas razonables para que se supriman o rectifiquen sin dilación los datos inexactos. Chile converge, añadiendo "completos" y "pertinentes" en relación con proveniencia y fines. En la OCDE, "*Data Quality Principle*" exige que los datos sean relevantes para los fines y, en la medida necesaria, exactos, completos y actualizados[71].

La comparación muestra que Chile combina formulaciones europeas y OCDE. En instrumentos interamericanos, la calidad también aparece ligada a exactitud y actualización, y se considera condición para evitar decisiones injustas. En la práctica europea, la calidad se vincula con derechos de rectificación y con obligaciones de notificar a terceros que recibieron datos, lo que también existe en el artículo 6 chileno.

Un aspecto comparado emergente es la calidad en datos inferidos y perfiles. El RGPD no distingue explícitamente, pero la doctrina y algunas decisiones regulatorias han enfatizado que inferencias pueden ser "datos personales" y deben cumplir con los requisitos de exactitud y transparencia. Respecto del riesgo en DPIAs se sugiere que la calidad de datos y la transparencia sobre inferencias son factores relevantes para evaluar riesgos a derechos. En Chile, el artículo 8° bis y el derecho de acceso a la "lógica aplicada" abren espacio para discutir calidad y explicación en contextos de perfilamiento.

7.4. Relaciones sistemáticas dentro de la Ley 21.719

La calidad se operacionaliza mediante el derecho de rectificación (artículo 6) y el deber de comunicar la rectificación a quienes hayan recibido datos,

[71] OECD (2013).

salvo imposibilidad o esfuerzo desproporcionado. Además, el derecho de supresión (artículo 7) incluye supuestos de datos "caducos", lo que se conecta con actualidad y pertinencia.

El deber de información (artículo 14 ter) y el derecho de acceso (artículo 5) contribuyen a calidad al permitir que el titular conozca origen, finalidad y período de tratamiento; sin información, el titular no puede detectar errores. La transparencia es, por tanto, condición funcional de la calidad.

En decisiones automatizadas (artículo 8° bis), la calidad adquiere especial relevancia: si una decisión produce efectos jurídicos o afecta significativamente, el riesgo de daño por datos inexactos es alto, lo que puede activar evaluación de impacto (artículo 15 ter, letra a) y exigir medidas de mitigación, entre ellas controles de calidad y mecanismos de revisión humana.

Finalmente, en el régimen de responsabilidad, datos inexactos pueden generar daños patrimoniales o morales y gatillar responsabilidad civil o administrativa. La Agencia, al sancionar, podrá considerar la falta de controles de calidad como infracción a principios y deberes, especialmente si el responsable no adoptó medidas razonables para rectificar o suprimir sin dilación.

8. Responsabilidad

8.1. Contenido normativo del artículo 3°

El artículo 3°, letra e), dispone que quienes realicen tratamiento serán "legalmente responsables" del cumplimiento de los principios del artículo 3° y de las obligaciones y deberes conforme a la ley. Este principio expresa, en un enunciado, que el régimen no es meramente programático: el incumplimiento tiene consecuencias jurídicas y, además, que la responsabilidad es transversal respecto de principios y deberes. La redacción no se limita a "cumplir", sino que atribuye responsabilidad legal por el cumplimiento.

8.2. Perspectiva doctrinal

La "responsabilidad" en protección de datos debe distinguirse de "responsabilidad" en sentido civil clásico. Aquí funciona como principio de gobernanza y de imputación: identifica al sujeto que decide fines y medios (responsable) como eje de deberes, aun cuando delegue operaciones a

encargados. En el modelo europeo, esto se denomina "*accountability*" o "responsabilización", de acuerdo con lo que señala el artículo 5(2) del RGPD.

Estepa[72] describe la responsabilidad proactiva como un cambio de paradigma: desde un régimen que presume buena fe y reacciona ante infracciones, hacia uno que exige gestión preventiva y demostrable del cumplimiento. La responsabilidad se vuelve "informadora" del régimen, pues reorganiza la relación entre norma, organización y control. En este modelo, el cumplimiento no se agota en evitar sanciones; se convierte en un deber estructural de implementar políticas, registros, evaluaciones, contratos con encargados, y mecanismos internos de control.

Desde una perspectiva teórica, la responsabilidad proactiva puede ser vista como una "internalización" de estándares: el derecho transfiere parte del trabajo normativo a las organizaciones, exigiéndoles traducir principios en procedimientos concretos. Este fenómeno es típico de regulaciones de riesgo (*compliance*, seguridad, protección ambiental). En datos, la responsabilidad se articula con la evaluación de impacto, con privacidad desde el diseño, y con modelos de prevención certificados, introduciendo una dimensión cuasi-regulatoria basada en controles internos.

La responsabilidad también cumple una función de asignación de cargas de prueba. Cuando el responsable debe acreditar licitud, existencia de medidas de seguridad o cumplimiento de deberes, se reconoce que el titular carece de acceso a la información organizacional. Por ello, la responsabilidad es condición de efectividad: sin inversión de carga argumental, los derechos del titular serían ilusorios.

En suma, la responsabilidad es el principio que convierte el catálogo del artículo 3° en un programa de cumplimiento exigible. Sin responsabilidad, los principios serían meros enunciados de valores. Con responsabilidad, se transforman en criterios de imputación y de diseño institucional.

8.3. Derecho comparado

El RGPD contiene una disposición explícita: artículo 5(2) ("*The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1*"), conocida como *accountability*. Chile no copia literalmente esta frase, pero incorpora dos equivalentes funcionales: (i) en licitud y lealtad, el deber de acreditar licitud; y (ii) en responsabilidad, la afirmación de responsabilidad legal por cumplimiento de principios y obligaciones. Esta

[72] Estepa (2022:67).

combinación sugiere que la *accountability* está distribuida en el texto chileno, en vez de concentrada en una sola frase.

La OCDE[73] incluye *accountability* como principio transversal: el responsable de datos debería ser responsable de cumplir medidas que den efecto a los principios y debe estar preparado para demostrarlo. El Convenio 108 también refuerza el rol de responsabilidad, especialmente al exigir medidas adecuadas y controles independientes. En el mundo iberoamericano, varias reformas han incorporado expresamente "responsabilidad demostrada" y obligaciones de documentación, siguiendo el modelo europeo. La comparación muestra, por tanto, que Chile se alinea con una tendencia global hacia la "*compliance-based regulation*" en datos.

En Alemania, la lógica de *accountability* se expresa tanto en el RGDP como en la práctica de autoridades y guías de cumplimiento, destacando documentación y evaluación de riesgos. En Francia e Italia, autoridades enfatizan que el respeto a principios del artículo 5 RGPD debe ser demostrable y que el responsable debe mantener registros de tratamiento y justificar decisiones. Esta convergencia comparada sugiere que la Agencia chilena probablemente exigirá evidencias (políticas, registros, DPIAs, contratos) como parte esencial de su fiscalización.

8.4. Relaciones sistemáticas dentro de la Ley 21.719

La responsabilidad se despliega en múltiples obligaciones específicas del Título IV. Este conjunto conforma una "arquitectura de *compliance*" que materializa el principio.

La evaluación de impacto (artículos 15 ter) es una manifestación paradigmática de responsabilidad proactiva: obliga a anticipar riesgos y a diseñar mitigaciones antes de iniciar tratamientos de alto riesgo. La consulta a la Agencia en caso de alto riesgo residual refuerza la lógica de responsabilidad supervisada.

El régimen sancionatorio (artículos 34 y ss.) traduce responsabilidad en consecuencias: infracciones leves, graves y gravísimas con multas y otras medidas. Además, la existencia de modelos de prevención certificados y un Registro Nacional de Sanciones y Cumplimiento (definición legal de "Registro") sugiere que la responsabilidad se conectará con incentivos de cumplimiento: certificaciones, atenuantes, y reputación regulatoria.

[73] OCDE (2013).

Por último, la responsabilidad debe leerse junto con las definiciones de responsable y tercero mandatario o encargado, y con el tratamiento por órganos públicos (artículos 22 y ss.). La responsabilidad delimita quién responde ante el titular y ante la Agencia, aunque existan múltiples actores en la cadena de tratamiento (proveedores tecnológicos, subencargados, etc.).

III. Síntesis

La reforma introducida por la Ley 21.719 sitúa a los principios del artículo 3° como el núcleo estructurante del nuevo derecho chileno de protección de datos. El catálogo se alinea con estándares internacionales consolidados —particularmente con el artículo 5 del GDPR, el Convenio 108+ y las Directrices OCDE— pero introduce opciones de técnica legislativa propias, como la separación de seguridad y confidencialidad, y la integración de minimización y conservación bajo proporcionalidad.

Desde un punto de vista dogmático, los principios cumplen funciones múltiples: delimitan el poder de tratamiento, informan la interpretación de reglas y excepciones, y se convierten en estándares de diligencia organizacional. La incorporación expresa de exigencias de acreditación y de responsabilidad legal muestra que el legislador adopta una lógica de cumplimiento demostrable, propia de regulaciones basadas en riesgo.

Desde el derecho comparado, la experiencia europea sugiere que la efectividad de los principios depende decisivamente de su densificación por autoridades independientes y por jurisprudencia, mediante guías, criterios de compatibilidad, estándares de transparencia, y parámetros de seguridad proporcionales al riesgo. En Chile, la Agencia tendrá un rol decisivo en traducir principios en prácticas verificables, evitando tanto un formalismo vacío (*compliance* de papel) como una indeterminación que debilite la seguridad jurídica.

Finalmente, el análisis sistemático muestra que cada principio se proyecta en deberes específicos (artículos 14 y ss.), derechos del titular (artículos 4 y ss.) y herramientas preventivas (artículo 15 ter). En la medida en que responsables y encargados internalicen esta arquitectura en sus procesos —mapeo de tratamientos, documentación de bases de licitud, diseño por defecto, gestión de incidentes y evaluación de impactos— los principios podrán cumplir su promesa normativa: transformar la protección de datos en un régimen efectivo de control del poder informacional, compatible con innovación y circulación legítima de información.

Catálogo de principios

Principio (art. 3°)	Contenido normativo (núcleo)	Deberes/controles típicos del responsable	Evidencias y respaldos (accountability) esperables
a) Licitud y lealtad	Tratamiento sólo de manera lícita y leal; deber reforzado: el responsable debe poder acreditar la licitud del tratamiento.	Inventario de bases de legitimidad por finalidad; evaluación de licitud ex ante; evitar prácticas engañosas; gobernanza de consentimiento y contratos.	Registro de tratamientos; matriz "base legal/ finalidad"; cláusulas de información y consentimiento; contratos con contrapartes y prestadores; auditorías internas.
b) Finalidad	Recolección con fines específicos, explícitos y lícitos; tratamiento limitado a dichos fines. Prohibición de finalidad distinta, con excepciones: i. compatibilidad; ii. relación contractual/ precontractual coherente; iii. nuevo consentimiento o habilitación legal.	Definir finalidades por capas; control de cambios de finalidad; evaluación de compatibilidad; gestión de renovación de consentimiento	Política de finalidades; evaluación de compatibilidad documentada; registro histórico de cambios; registro de consentimiento; DPIA (evaluación de impacto en la protección de datos) cuando corresponda.
c) Proporcionalidad	Criterio estricto (reducido al mínimo): tratar sólo datos necesarios, adecuados y pertinentes para los fines. Retención: conservar sólo por el tiempo necesario; luego suprimir o anonimizar; retención por lapso superior requiere ley o consentimiento.	Diseño de formularios y recolección mínima; revisiones periódicas de pertinencia; políticas de retención y borrado; anonimización/ pseudonimización.	Inventario de datos por finalidad; política de retención con plazos; bitácoras de borrado/anonimización; análisis de necesidad/ adecuación.
d) Calidad	Datos exactos, completos, actuales y pertinentes respecto de su proveniencia y fines.	Validaciones; mecanismos de actualización; controles de duplicidad; procesos de rectificación y trazabilidad.	Indicadores de calidad; logs de corrección; procedimientos de actualización; pruebas de integridad.
e) Responsabilidad	Responsabilidad legal por cumplimiento de principios y obligaciones/ deberes de la ley (accountability).	Modelo de cumplimiento; asignación de roles; capacitación; gestión de riesgos; auditorías.	Políticas internas; reportes de auditoría; evidencias de capacitación; matrices de riesgos; documentación de decisiones.

f) Seguridad	Garantizar estándares adecuados de seguridad; protección frente a tratamiento no autorizado o ilícito, y frente a pérdida/filtración/ daño/ destrucción accidental. Medidas apropiadas según tratamiento y naturaleza de los datos.	Gestión de accesos; cifrado; segregación; respaldo; monitoreo; gestión de vulnerabilidades; respuesta a incidentes; seguridad por diseño/por defecto.	Evaluaciones de riesgo; políticas de seguridad; controles técnicos; evidencias de test o pruebas de control; planes de respuesta; registros de incidentes.
g) Transparencia e información	Deber de entregar al titular la información necesaria para el ejercicio de sus derechos; políticas y prácticas de tratamiento permanentemente accesibles, precisas, claras, inequívocas y gratuitas.	Avisos de privacidad por capas; canales de atención; publicación de políticas; trazabilidad de comunicaciones; atención de solicitudes.	Registro de versiones de políticas; repositorio público; métricas de atención; copias de avisos entregados; evidencia de accesibilidad.
h) Confidencialidad	Deber de secreto/ confidencialidad para el responsable y quienes accedan a datos; controles y medidas adecuadas; subsiste tras concluir la relación con el titular.	Acuerdos de confidencialidad; controles de acceso; segregación; monitoreo; gestión de terceros; cláusulas post-contractuales.	Acuerdos de confidencialidad y cláusulas laborales; bitácoras de acceso; registros de autorización; controles de terceros; sanciones internas.

Capitulo 5
Titulares de la protección de datos

I. Titulares

Los titulares del derecho de protección de datos se encuentran definidos en el artículo 2 ñ) de su versión modificada por la Ley 21.719 que señala:

> ñ) Titular de datos o Titular: persona natural, identificada o identificable, a quien conciernen o se refieren los datos personales.

En este sentido, la norma es amplia y dispensa protección a personas naturales identificadas y también cuando ellas detentan la condición de identificables, concepto que ya está descrito en el mismo artículo en el numeral f) al definir los datos personales y allí se indica:

> 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.

Por consiguiente, el ámbito de protección está claramente delimitado y ello evita ambigüedades respecto de personas jurídicas, que pueden invocar otras normas legales, pero no la titularidad directa del derecho de protección de datos. La ley, por tanto, tutela en primer término a individuos, coherente con el estándar internacional que concibe el derecho de protección de datos como resguardo de la persona frente a asimetrías informacionales y de poder. Los derechos que se les otorga a los titulares son prerrogativas subjetivas de carácter personal e irrenunciable. La ley, por ende, reconoce expresamente los derechos de acceso, rectificación, supresión, oposición, portabilidad y bloqueo (Ley 21.719, artículos 5°–8° ter). La configuración legal refuerza la tutela como estatuto de orden público, cerrando la puerta a cláusulas abusivas que pretendan exigir renunciar a derechos o someterlos a condiciones contractuales desequilibradas para las partes del contrato. La

irrenunciabilidad se alinea con la lógica de derechos fundamentales, pero plantea interrogantes prácticos (por ejemplo, "renuncias" funcionales vía diseño oscuro). De ahí la relevancia de los deberes de transparencia y de mecanismos sencillos para ejercer esta clase de derechos.

Un aspecto relevante para considerar es la tutela de titular en clave relacional, es decir, ver el contexto más allá del individuo de forma aislada. La tutela de datos no se agota en el control individual, vale decir, bajo la lógica sólo del consentimiento, aunque éste sea la regla general en la ley reformada. Los datos son relacionales (afectan a terceros, revelan inferencias algorítmicas, generan externalidades). La ley incorpora parcialmente esta dimensión mediante deberes de seguridad, diseño, transparencia y sanciones; pero aún dependerá de cómo se aborde la elaboración de perfiles, la inferencia algorítmica y la interoperabilidad de bases públicas y privadas. La tutela moderna exige, además de derechos individuales, una gobernanza del ecosistema de datos.

II. Niños, niñas y adolescentes

1. Consideraciones generales

La Convención sobre los Derechos del Niño -CDN- instauró un nuevo paradigma en el reconocimiento de los NNA como sujetos de derecho, lo que "implica que se le reconocen derechos autónomos, con capacidad para ejercerlos por sí mismo, de acuerdo con la evolución y desarrollo de sus facultades"[74]. Entre estos, "NNA gozan, en tanto que son personas, del derecho a la protección de sus datos personales, el cual se traduce en la debida observancia de una serie de principios y derechos"[75].

Dentro del catálogo de derechos fundamentales de niñez y adolescencia que el pacto internacional antes referido establece no se encuentra el derecho a la protección de datos personales. Sin embargo, éste consagra en su artículo 16[76] el derecho a la intimidad, los que, si bien autónomos, se encuentran

[74] Gómez (2018: 118).

[75] Ornelas (2010: 171).

[76] Artículo 16. "1. Ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y a su reputación.
2. El niño tiene derecho a la protección de la ley contra esas injerencias o ataques".

en íntima conexión. En torno a la vinculación del derecho a la intimidad con el derecho a la protección de datos personales la doctrina ha sostenido, "[C]on el primero, se protege la confidencialidad de la información relativa a un individuo, mientras que con el segundo se garantiza el buen uso de la información relativa a un sujeto, una vez que ésta ha sido revelada a un tercero, ya que el dato confesado no es por ello público y, en consecuencia, no puede circular libremente"[77].

En cuanto a la fisonomía propia del derecho a la protección de datos personales el TCE, en el fundamento de derecho 7 de su sentencia de pleno 27/2020, de 24 de febrero ha señalado,

> […] el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.

Es preciso considerar a los NNA nativos digitales[78], que corresponde a aquel grupo de personas "que han ido creciendo con un uso de internet ya consolidado, y en buena medida dependientes de las nuevas tecnologías"[79], encontrando en estas el medio para satisfacer sus "necesidades de entretenimiento, información, comunicación e incluso de formación"[80].

El avance de las Tecnologías de la Información y de las Comunicaciones y de los entornos en los que éstas se desenvuelven, han ofrecido nuevas

[77] Ravetllat y Basoalto (2021: 115).

[78] Casadei (2025:7).

[79] Acedo y Platero (2016: 71).

[80] Lorente (2015: 207)

oportunidades para el desarrollo y efectivización de los derechos de NNA, aunque no ha sido ajeno a una serie de riesgos a su integridad[81], más aún cuando su uso se inicia en edades cada vez más tempranas, llegando hoy al promedio de los 7 años de edad[82].

El entorno digital mantiene disponible la información personal proporcionada y los datos publicados pudiendo otras personas interactuar con estos e incluso replicarlos, lo que encierra peligros que niños y adolescentes suelen no percibir: acceso a su intimidad personal, manipulación de información, su uso indebido o indeseable, cuestiones que pueden afectarle no tan solo en el presente sino también en el futuro[83]; y supone, además, el tratamiento automatizado por las empresas responsables de los datos personales y propias preferencias que los titulares difunden.

En el escenario descrito, los NNA ven profundizada su vulnerabilidad tanto por desconocimiento de cuestiones técnicas, como por tratarse de un sistema regido desde la adultez exigiendo por ello una protección prioritaria[84], la que ha sido abordada tanto en el ámbito internacional como en los ordenamientos jurídicos internos.

Consciente de la expansión del uso de la tecnología y su utilización masiva por NNA, el Comité de los Derechos del Niño, en su Observación General N°25, relativa a los derechos de los niños en relación con el entorno digital, ha explicado "la forma en que los Estados partes deben aplicar la Convención en relación con el entorno digital"[85], señalando los principios de no discriminación, interés superior del niño, derecho a la vida, a la supervivencia y al desarrollo y de respeto a las opiniones del niño conforme la evolución de sus facultades, como "una lente a través de la que debe considerarse el ejercicio de todos los demás derechos previstos en la Convención"[86], sirviendo de guía para garantizar la efectividad de los derechos de los niños en el entorno digital, dando cuenta que este entorno "no fue diseñado en un principio para los niños, sin embargo, desempeña un papel importante en su vida"[87]. De esta manera resulta clarificador que no solo el derecho a la protección de datos personales puede verse expuesto en el entorno digital sino también otros derechos de la personalidad involucrados en el constante e ilimitado

[81] Álvarez (2020: 52 – 54).

[82] Defensoría de la Niñez (2024: 4).

[83] Riveros y López (2025: 277).

[84] Ordóñez y Calva (2020:109).

[85] Comité de los Derechos del Niño (2021: 2), parágrafo 7.

[86] Comité de los Derechos del Niño (2021: 2), parágrafo 8.

[87] Comité de los Derechos del Niño (2021: 3), parágrafo 12.

flujo de información que encierra, como el derecho a la identidad digital, el derecho a la imagen, honra, honor y privacidad.

Conforme la referida Observación General, el entorno digital abarca "las tecnologías de la información y las comunicaciones, incluidas las redes, los contenidos, los servicios y las aplicaciones digitales, los dispositivos y entornos conectados, la realidad virtual y aumentada, la inteligencia artificial, la robótica, los sistemas automatizados, los algoritmos y el análisis de datos, la biometría y la tecnología de implantes"[88].

En el espacio de América Latina y El Caribe, cabe mencionar el Memorándum de Montevideo sobre protección de datos personales y la vida privada en la redes sociales en internet, en particular de NNA, que proclama una serie de sugerencias adoptadas en el Seminario Derechos, Adolescentes y Redes Sociales en Internet, realizado en la ciudad de Montevideo los días 27 y 28 de julio de 2009, entre ellas respecto el marco legal, indicando que la creación, reforma o armonización normativa debe hacerse tomando como consideración primordial el interés superior de NNA[89], debiendo comprender, sea directamente o a través de sus representantes legales, su derecho a solicitar el acceso a la información que sobre sí mismos se encuentre en bases de datos públicas o privadas, así como a la rectificación o cancelación de dicha información cuando resulte procedente y la oposición a su uso para cualquier fin[90].

> En el ámbito regional europeo, respecto NNA, su párrafo 38 señala, Los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales. Dicha protección específica debe aplicarse en particular, a la utilización de datos personales de niños con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario, y a la obtención de datos personales relativos a niños cuando se utilicen servicios ofrecidos directamente a un niño.

Un tema cardinal en la materia es determinar la edad o el grado de madurez para manifestar su voluntad en orden a la utilización y tratamiento de sus datos personales. El RGPD dedica su artículo 8 a establecer las condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información, disponiendo:

---

[88] Comité de los Derechos del Niño (2021: 1), parágrafo 2.

[89] Memorándum de Montevideo (2009: 11), apartado 5.

[90] Memorándum de Montevideo (2009: 9), apartado 3.8.

> 1. Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó. Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años.

2. NNA y derecho a la protección de datos personales en Chile

El panorama legal interno del derecho a la protección de datos personales se conforma por las disposiciones contenidas en la Ley 21.430, sobre garantías y protección integral de los derechos de la niñez y adolescencia y, la Ley 19.628 con la reciente modificación de la Ley 21.719.

Entre los derechos que, en clave de garantía, consagra la Ley 21.430 en el párrafo segundo de su Título II, se encuentran el derecho a la vida privada y a la protección de datos personales y el derecho a la honra, intimidad y propia imagen[91]. No obstante constituir el sustrato de un derecho en sí mismo, pueda ser tratada, además, como un dato personal y sujeta a las leyes sobre protección de datos[92].

El artículo 33 de la Ley 21.430 consagra el derecho a la vida privada y a la protección de datos personales, disponiendo:

> Todo niño, niña y adolescente tiene derecho a desarrollar su vida privada. Ningún niño, niña o adolescente podrá ser objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia.
>
> Los niños, niñas y adolescentes tienen derecho a la protección de sus datos personales, así como a impedir su tratamiento o cesión, según lo establecido en la legislación vigente.
>
> Cuando el tratamiento esté referido a datos de niños, niñas y adolescentes, la información dirigida a ellos deberá expresarse en un lenguaje que les sea fácilmente comprensible.

[91] Riveros y Arratia (2025: 40); Gil (2013: 63).

[92] Donoso y Reusser (2021: 239).

> Los funcionarios públicos, las organizaciones de la sociedad civil que se relacionen con la niñez y su personal deberán guardar reserva y confidencialidad sobre los datos personales de los niños, niñas y adolescentes a los que tengan acceso, a menos que su divulgación resulte indispensable para la protección de sus derechos y siempre que se tomen los resguardos necesarios para evitar un daño mayor.

La disposición, conforme el objeto de la Ley 21.430 -artículo 1-, interpretada desde la doctrina de la protección integral de niñez y adolescencia, apunta a otorgar efectividad a las prerrogativas que reconoce -artículo 12-, en conjugación con los principios consagrados en el párrafo primero del título II, entre estos, el interés superior del niño -artículo 7- y su autonomía progresiva -artículo 11-.

El interés superior de niños, niñas o adolescentes impone que en cualquier decisión que los involucre, cualquiera sea el ámbito en que adopte, se deben evaluar todos los elementos de la situación concreta apuntando a la máxima satisfacción posible de sus derechos y garantías.

La recolección de datos, su tratamiento y la posibilidad de que estos se repliquen en el tiempo pudiendo tener impacto no solo actual, lleva a tener especialmente presentes las circunstancias que, sin carácter exhaustivo, señala el inciso final del artículo 7 para determinar el interés superior del niño, niña o adolescente en cada caso concreto:

> **a)** Los derechos actuales o futuros del niño, niña o adolescente que deban ser respetados, promovidos o protegidos por la decisión de la autoridad.
>
> **b)** La opinión que el niño, niña o adolescente exprese, cuando ello sea posible conforme a su edad, grado de desarrollo, madurez y/o su estado afectivo si no pudiere o no quisiere manifestarla.
>
> **c)** La opinión de los padres y/o madres, representantes legales o de quien lo tuviere legalmente a su cuidado, salvo que sea improcedente.
>
> **d)** El bienestar físico, mental, espiritual, moral, cultural y social del niño, niña o adolescente.
>
> **e)** La identidad del niño, niña o adolescente y las necesidades que de ella se derivan, sean éstas físicas, emocionales, sociales, culturales o de origen étnico.
>
> **f)** La autonomía del niño, niña o adolescente y su grado de desarrollo.
>
> **g)** Cualquier situación de especial desventaja en la que se encuentre el niño, niña o adolescente que haga necesaria una protección reforzada

para el goce y ejercicio efectivos de sus derechos.

h) La necesidad de estabilidad de las soluciones que se adopten para promover la efectiva integración y desarrollo del niño, niña o adolescente considerando su entorno de vida.

i) Otras circunstancias que resulten pertinentes en el caso concreto que se conoce, tales como los efectos probables que la decisión pueda causar en su desarrollo futuro.

Conforme el artículo 11 de la Ley 21.430, el principio de autonomía progresiva apunta a que NNA ejerzan sus derechos directamente "en consonancia con la evolución de sus facultades, atendiendo a su edad, madurez y grado de desarrollo que manifieste, salvo que la ley límite este ejercicio, tratándose de derechos fundamentales". Además, la Ley 21.719 ha introducido en nuestro sistema reglas respecto el ejercicio del derecho a la protección de datos personales de NNA, aspecto en el que profundizaremos seguidamente.

La especial vulnerabilidad que afecta a NNA el tratamiento de sus datos personales ha sido advertida por la Corte Suprema en sus sentencias de 06 de enero de 2025, causa rol 18.566-2024 y 07 de enero de 2025, causa rol 35.760-2024.

Ambas sentencias revocan los fallos de la Corte de Apelaciones de Santiago y Valparaíso, respectivamente, dando lugar a las acciones constitucionales deducidas por la recopilación, almacenamiento y tratamiento de datos biométricos de menores de edad a través del escaneo de sus iris efectuado por la empresa Worldcoin SpA, considerándolo una clara infracción a lo dispuesto por el artículo 33 de la Ley 21.430 y por la Ley 19.628 respecto el otorgamiento de consentimiento válido, vulnerando las garantías constitucionales contenidas en el artículo19 N°1 y 4 de la CPR y el derecho a la protección de datos personales.

La sentencia dictada en causa rol 18.566-2024, en su considerando cuarto señala:

> […] consta del mérito de la acción constitucional intentada que lo impugnado, en lo medular, es el almacenamiento y tratamiento de los datos personales de la menor referida en autos, lo que no es una acción única en el tiempo, sino que se mantendría en la actualidad […].
>
> Para continuar en su considerando noveno indicando:
>
> Que, conforme se colige de lo señalado en autos, mediante la acción de escaneo de iris se han recopilado los datos biométricos de la menor referida, sin embargo, esto se ha materializado sin el consentimiento

de aquélla, aspecto fundamental a estos efectos. Al respecto, es necesario tener en consideración que el hecho impugnado requiere de un examen particular al involucrar a una menor de edad, peculiaridad que la ubica en un ámbito de protección reforzada respecto del uso de sus datos personales y más aún, de la forma de obtener y almacenar los mismos.

Concluyendo en el considerando siguiente:

Décimo: Que, en este orden de ideas, no existe controversia que las recurridas obtuvieron el escaneo del iris y el almacenamiento de datos de la menor señalada, en clara infracción del Artículo 33 de la Ley N°21.430, al no proporcionarle la información mínima para que ella estuviese en condiciones de haber impedido el uso de sus datos personales, por lo que no era posible para ella aquilatar la envergadura de aquello a lo que estaba accediendo.

A lo que se viene diciendo, hay que agregar, que el mandato de no injerencia en la vida privada de un menor a que se refiere expresamente la norma que se viene citando, es de cumplimiento transversal, o sea para cualquier persona natural o jurídica que se relacione con menores de edad, en consecuencia, las recurridas en conocimiento de la ley, que se presume conocida por todos, debieron inhibirse de recopilar y almacenar los datos biométricos de la menor de edad, puesto que estos son datos sensibles con una protección reforzada en el caso de aquélla, conforme lo dispone las normas legales y constitucionales citadas precedentemente.

En lo que atañe al otorgamiento del consentimiento por parte de una persona menor de edad, la sentencia dictada en causa rol 35.760-2024 en su considerando octavo indica:

Que, conforme se colige de lo señalado en autos, mediante la acción de escaneo de iris se han recopilado los datos biométricos del menor de edad protegido, sin embargo, esto se habría materializado sin contar con un consentimiento legamente otorgado, por sus padres o representantes legales o por quien tiene a su cargo el cuidado personal del menor, aspecto fundamental a estos efectos. Al respecto, es necesario tener en consideración que el hecho impugnado requiere de un examen particular al involucrar a un menor de edad, peculiaridad que lo ubica en un ámbito de protección reforzada respecto del uso de sus datos personales y más aún, de la forma de obtener y almacenar los mismos.

Agregando en su considerando noveno,

> […] no cabe si no concluir que, ante el escaneo del iris y el almacenamiento de datos del adolescente, en clara infracción del Artículo 33 de la Ley N°21.430, al no proporcionarle la información mínima para que le fuera posible entender la envergadura de aquello a lo que estaba accediendo, y de las normas de la Ley N°19.628, respecto del otorgamiento del consentimiento válidamente, pues éste no fue otorgado por sus padres o representantes legales o por quien tiene a su cargo el cuidado personal del niño o niña, el tratamiento de datos personales del menor de autos carece de toda base legal.

Respecto la empresa recurrida que efectúa la recopilación de datos biométricos para una empresa mandante extranjera, en el considerando décimo, indica:

> "[…] En consecuencia, siendo la recurrida la encargada de recopilar los datos biométricos, necesariamente debía dar cumplimiento a la normativa verificando la edad de los usuarios, informando debidamente sobre sus riesgos y recopilando un consentimiento válidamente emitido".

Como señalamos con anterioridad, ha sido la Ley 21.719 la que, complementando las disposiciones de la Ley 19.628, ha venido a regular dentro de su Título II, en el párrafo tercero dedicado al tratamiento de categorías especiales de datos personales, lo relativo a los datos personales de NNA. Así, el artículo 16 quáter ha venido a dar contenido al artículo 33 de la Ley 21.430 al prescribir, "Los niños, niñas y adolescentes tienen derecho a la protección de sus datos personales, así como a impedir su tratamiento o cesión, según lo establecido en la legislación vigente". El artículo 16 quáter dispone:

> Datos personales relativos a los niños, niñas y adolescentes. El tratamiento de los datos personales que conciernen a los niños, niñas y adolescentes, sólo puede realizarse atendiendo al interés superior de éstos y al respeto de su autonomía progresiva.
>
> Cumpliéndose la exigencia establecida en el inciso anterior, para tratar los datos personales de los niños y niñas se requiere el consentimiento otorgado por sus padres o representantes legales o por quien tiene a su cargo el cuidado personal del niño o niña, salvo que expresamente lo autorice o mandate la ley.
>
> Los datos personales de los adolescentes se podrán tratar de acuerdo a las normas de autorización previstas en esta ley para los adultos, salvo lo dispuesto en el inciso siguiente.

> Los datos personales sensibles de los adolescentes menores de dieciséis años sólo se podrán tratar con el consentimiento otorgado por sus padres o representantes legales o quien tiene a su cargo el cuidado personal del menor, salvo que expresamente lo autorice o mandate la ley.
>
> Para los efectos de esta ley, se consideran niños o niñas a los menores de catorce años, y adolescentes, a los mayores de catorce y menores de dieciocho años.
>
> Constituye una obligación especial de los establecimientos educacionales y de todas las personas o entidades públicas o privadas que traten o administren datos personales de niños, niñas y adolescentes, incluidos quienes ejercen su cuidado personal, velar por el uso lícito y la protección de la información personal que concierne a los niños, niñas y adolescentes.

Para el tratamiento de sus datos personales de NNA, la disposición establece dos exigencias:

> 1° Atención al interés superior del niño y respeto de su autonomía progresiva.
>
> Se trata de un contenido innovador en la materia y coherente con las disposiciones de la Ley 21.430, estableciendo una garantía base para la tutela del derecho a la protección de datos personales.
>
> 2° Contar con el consentimiento libre, específico, inequívoco e informado necesario.

El que se determina en el siguiente esquema:

<table>
<tr><th rowspan="2">Niños y Niñas
Personas menores de 14 años</th><th colspan="3" rowspan="2">Adolescentes
Personas mayores de 14 y menores de 18 años</th></tr>
<tr></tr>
<tr><td rowspan="4">Regla general: requiere el consentimiento otorgado por sus padres o representantes legales o por quien tiene a su cargo el cuidado personal

Excepción: casos expresamente autorizados por la ley</td><td>Datos personales mayores 14 y menores 18 años</td><td colspan="2">Datos personales sensibles</td></tr>
<tr><td rowspan="3">Normas previstas para los adultos</td><td>mayores 14 y menores 16 años</td><td>Mayores de 16 y menores de 18 años</td></tr>
<tr><td rowspan="2">Regla general: requiere el consentimiento otorgado por sus padres o representantes legales o quien tiene a su cargo el cuidado personal

Excepción: casos expresamente autorizados por la ley</td><td rowspan="2">Normas previstas para los adultos</td></tr>
<tr></tr>
</table>

Frente a la complejidad en torno a la determinación de la validez del consentimiento de NNA, la doctrina ha sugerido acompañar el grado de madurez de un criterio de edad por ser más objetivo, sencillo e igualitario[93].

La regulación chilena optó por seguir el estándar europeo, adoptando un sistema mixto que incorpora límites objetivos de edad para complementar la autonomía progresiva. Es de considerar, además, que el inciso primero del referido artículo 11, por excepción, reconoce que la ley puede limitar el ejercicio directo de los derechos de NNA tratándose de derechos fundamentales, caso del derecho a la protección de datos personales.

Ahora bien, respecto los adolescentes a quienes la Ley 21.719 reconoce la posibilidad de otorgar consentimiento y autorización en forma directa para el tratamiento de sus datos personales, siguiendo la corriente doctrinal que, para el ejercicio de derechos extrapatrimoniales, observa en los rangos etarios dispuestos por la ley el establecimiento de presunciones *iuris tantum* respecto la capacidad de ejercicio de los adolescentes, el complemento que aporta el grado de madurez en el examen de la situación concreta permitiría desvirtuar la presunción legal, aportando un elemento dinámico al componente objetivo y estático de la edad[94], admitiendo prueba en contrario en resguardo del derecho a la protección de datos personales, evitando con ello el posible grado de arbitrariedad en la resolución de conflictos relativos a la valoración del consentimiento de personas menores de edad.

Para los casos en que la ley reconoce autonomía y grado de madurez suficiente a los adolescentes para el otorgamiento de su autorización -mayores de 14 y menores de 18 años respecto el tratamiento de sus datos personales; y, mayores de 16 y menores de 18 años en torno a sus datos personales sensibles- resulta indispensable que pueda conocer aquello en que está consintiendo, con lo que la información previa y detallada se convierte en una condición esencial para contribuir a conformar el consentimiento libre e informado que se requiere para el otorgamiento de una declaración de voluntad válida. En este sentido constituye un aporte la disposición contenida en el inciso tercero del artículo 33 de la Ley 21.430 al prescribir que la información dirigida a NNA "deberá expresarse en un lenguaje que les sea fácilmente comprensible".

En materia de consentimiento otorgado por personas menores de edad, una cuestión relevante es la verificación, por parte del responsable del

[93] Acedo y Platero (2016: 77 – 78 y 83); Ravetllat y Basoalto (2021: 129).

[94] León (2012:115); Acedo y Platero (2016: 78); Parra y Ravetllat (2019: 235); Ravetllat y Basoalto (2021: 129); Parra y Ravetllat (2023: 85-86); Álvarez y Riveros (2025: 94).

tratamiento de datos, de que la declaración de voluntad ha sido válidamente emitida, en la materia que analizamos, si cuenta con la edad para su otorgamiento o bien, el consentimiento ha sido dado por sus padres o representantes legales.

Respecto el tratamiento de datos personales NNA en el entorno virtual, la Observación General N°25 del Comité de los Derechos del Niño insta a los Estados parte a "exigir que las organizaciones que procesan esos datos verifiquen que el consentimiento es informado, consecuente y dado por el padre o cuidador del niño"[95], en los casos que las legislaciones internas así lo requieran.

El RGPD, en su artículo 8.2 señala, "El responsable del tratamiento hará esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible". La regulación europea no indica en qué consisten los esfuerzos razonables a que alude, por lo que consecuentemente cuentan con libertad para desarrollar los métodos que permitan cumplir con esta obligación de hacer en las operaciones que lleven a cabo, las que deberán ser proporcionales a la naturaleza y riesgos de las actividades de tratamiento de datos que desplieguen[96].

También en el ámbito europeo preciso es tener presente el Reglamento 2022/2065 del parlamento Europeo y del Consejo de la Unión Europea, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales que en su artículo 35, entre las medidas para la mitigación de los riesgos que deben aplicar los prestadores de plataformas en línea y de motores de búsqueda en línea de gran tamaño, indica: "j) la adopción de medidas específicas para proteger los derechos de los menores, incluidas herramientas de comprobación de la edad y de control parental, herramientas destinadas a ayudar a los menores a señalar abusos u obtener ayuda, según corresponda".

Reconociendo la importancia de un enfoque coherente a nivel de la Unión Europea, el Comité Europeo de Protección de Datos adoptó la Declaración 1/2025 sobre la determinación de la edad, enfatizando que "la comprobación de la edad es una solución para mejorar el bienestar de los niños en línea a través de un entorno digital seguro y adaptado a su edad, en consonancia con los derechos y principios digitales europeos"[97]. Determinación de edad refiere al "término genérico que engloba los métodos que se utilizan para determinar la edad o el intervalo de edad de una persona con distintos

[95] Comité de los Derechos del Niño (2021: 13), parágrafo 71.

[96] Ravetllat y Basoalto (2021: 134 - 135).

[97] Comité Europeo de Protección de Datos (2025: 1), párrafo 2.

niveles de confianza o certeza"[98], identificando tres categorías principales de la determinación de la edad: estimación de la edad; verificación de la edad; y, autodeclaración.

Centrada en los principios aplicables a los diferentes casos de uso en línea, en particular cuando, en virtud de obligaciones legales o de otro tipo, se prescribe una edad mínima para comprar productos y utilizar servicios que puedan perjudicar a los menores o para realizar actos jurídicos; y cuando exista un deber de diligencia de proteger a los menores (por ej., garantizar que los servicios se diseñen o se ofrezcan de una manera adaptada a su edad)[99], aborda prioritariamente los requisitos relativos a los principios fundamentales establecidos en el RGPD, señalando aquellos para que el diseño de la determinación de edad cumpla con la normativa: Disfrute pleno y efectivo de los derechos y libertades; Evaluación basada en el riesgo de la proporcionalidad de la determinación de la edad; Prevención de riesgos en materia de protección de datos; Limitación de la finalidad y minimización de datos; Eficacia de la determinación de la edad; Licitud, lealtad y transparencia; Decisiones automatizadas; Protección de datos desde el diseño y por defecto; Seguridad de la determinación de la edad; y, Responsabilidad proactiva.

La literatura apunta a la regulación norteamericana sobre protección en línea del derecho a la privacidad de las personas menores de edad de 1998, conocida como COPPA, como pionera respecto la identificación de mecanismos de verificación del consentimiento parental, entre los que se proponen proporcionar formularios de consentimiento a firmar por los representantes legales; facilitar un número telefónico gratuito o una video conferencia para que los representantes legales entren en contacto con el personal del responsable del tratamiento; enviar, con posteridad a la prestación del consentimiento, un mensaje por vía electrónica a los representantes legales para que confirmen su declaración de voluntad; comprobar la identidad de los representantes legales a través de bases de datos de identificación emitidas por el Gobierno; implantar un sistema de e-mail plus o de doble verificación que permita solicitar que los representantes indiquen su consentimiento en un mensaje de retorno; y requerir al representante legal, en conexión con una transacción monetaria, el uso de una tarjeta de crédito, de débito u otro sistema de pago en línea que proporcione notificación de cada transacción al titular de la cuenta principal[100].

[98] Comité Europeo de Protección de Datos (2025: 2), párrafo 3.

[99] Comité Europeo de Protección de Datos (2025: 2), párrafo 8.

[100] Ravettllat y Basoalto (2021: 136); Martínez (2020: 232 - 233).

Otras herramientas que se han identificado al efecto consisten en la utilización de perfiles de control de la actividad o la instalación de softwares específicos para la detección de la edad del usuario mediante la identificación de su lenguaje o fotos[101].

Considerando que con la Ley 21.719 se introduce en Chile un modelo institucional centrado en una autoridad de control especializada, la Agencia conforme las funciones y atribuciones que se le asignan en el artículo 30 bis de la Ley 19.628 modificada, deberá impartir las instrucciones a los responsables del tratamiento de datos respecto las medidas a adoptar, que constituyan los esfuerzos necesarios a su cargo para verificar que la declaración de voluntad sea válidamente emitida en el caso de personas menores de edad, considerando la naturaleza de los datos cuyo tratamiento efectúa y los riesgos asociados. Respecto del tratamiento de datos que por su naturaleza, alcance, contexto, tecnología utilizada o fines pueda producir un alto riesgo para los derechos de los titulares, el artículo 15 *ter* impone la obligación a los responsables de realizar una evaluación de impacto en protección de datos personales previo al inicio de sus operaciones.

El modelo de prevención de infracciones que en el artículo 48 prescribe la ley, conduce a que los responsables del tratamiento de datos personales deban también adoptar las acciones destinadas a prevenir la comisión de infracciones entre las que, con carácter grave, se encuentra el tratamiento de datos personales sin contar con el consentimiento del titular -artículo 34 ter a)-.

3. Tutela del derecho a la protección de datos personales de NNA

NNA son titulares del derecho a la protección de datos personales y de las facultades que en el comprenden: derecho de acceso, rectificación, supresión, oposición, portabilidad y bloqueo de sus datos personales, los que ejercerán en forma directa o a través de sus representantes legales siguiendo las reglas introducidas por la Ley 21.719.

Tratándose de datos relativos a personas menores de edad, la referida ley adiciona deberes en el responsable del tratamiento de datos personales, por ejemplo, en el artículo 14 sexies que dispone el deber de reportar vulneraciones a las medidas de seguridad, tratándose de NNA respecto sus datos personales sensibles, además de reportar a la Agencia por los medios más expeditos y sin dilaciones indebidas, deberá efectuar la comunicación a los

[101] Acedo y Platero (2016: 80); Barranco (2025: 62).

titulares, a través de sus representantes legales, la que se efectuará en un lenguaje claro y sencillo.

El derecho a la protección de datos personales encuentra protección mediante la acción de tutela constitucional. Ahora bien, respecto el daño provocado a NNA en su derecho a la protección de datos personales o en aquellas prerrogativas que lo conforman, cuenta con la vía de la responsabilidad civil franqueada en su artículo 47.

Tratándose de otro derecho de la personalidad incardinado con el derecho a la protección de datos personales que se vea lesionado, como el derecho a la identidad, honra, intimidad o propia imagen, el recurso a las reglas generales de la responsabilidad civil por daños[102], constituye también un medio de tutela para obtener el resarcimiento del daño sufrido. Relevante es considerar que el legislador nacional en el artículo 34 de la Ley 21.430 incluye su resguardo en el ámbito de las tecnologías de la información y las comunicaciones, sector que actualmente concentra un importante volumen de tratamiento de datos personales, lo que en el caso de NNA se advierte en las redes sociales a que acceden y en las que agregan información y contenidos. En el inciso final de la disposición, entre las sanciones a que alude, señala las civiles, "las que se verán agravadas cuando el afectado sea un menor de edad, conforme la legislación vigente". Desprendemos que el legislador ha querido con ello referirse al régimen general de la responsabilidad civil por daños[103], el que se verá agravado, cuestión que deberá ser ponderada por el juez que conozca de la causa por indemnización de perjuicios.

Encontrándose el derecho a la protección de datos de NNA consagrado en el artículo 33 de la Ley 21.430, cabe considerar que, ante su amenaza o vulneración, ya sea limitando o privando su ejercicio, por acción u omisión, resultará posible activar la tutela judicial y administrativa que este cuerpo normativo contempla.

Conforme los artículos 57 y 58 de la Ley 21.430, la protección comprende la preservación y restitución de derechos, así como su reparación, interviniendo en el plano judicial el tribunal de familia competente y en el administrativo, la oficina local de la niñez.

El artículo 60 establece, además, una acción de tutela administrativa de derechos, la que reconociendo una amplitud de sujetos activos, puede ser solicitada por el mismo niño, niña o adolescente afectado ante la Secretaria Regional Ministerial del Ministerio de Desarrollo Social y Familia, las

[102] Riveros y López (2025: 274).

[103] Ibáñez (2023: 916).

direcciones regionales del Servicio Nacional de Protección Especializada a la Niñez y Adolescencia o las Oficinas Locales de la Niñez "con el fin de que los órganos competentes tomen las medidas necesarias para hacer cesar la afectación de sus derechos"[104]. En los casos de amenaza o vulneración al derecho a la protección de datos personales la interacción necesaria deberá darse con la Agencia.

Para concluir, considerando la interacción de datos en el entorno digital, la Observación General N°25 de 2021 del Comité de los Derechos del Niño, en su parágrafo 44 insta a los Estados Parte a asegurarse "de que todos los niños y sus representantes conozcan y tengan a su disposición mecanismos de reparación judiciales y no judiciales adecuados y eficaces para abordar las violaciones de los derechos de los niños en el entorno digital". Para el organismo internacional una reparación adecuada "incluye la restitución, la compensación y la satisfacción y puede requerir una disculpa, una corrección, la eliminación de contenidos ilícitos, el acceso a servicios de recuperación psicológica u otras medidas"[105], teniendo en cuenta "la vulnerabilidad de los niños y la necesidad de actuar con rapidez a fin de detener los daños actuales y futuros"[106].

II. Otros Grupos Vulnerables

La *ratio legis* para proteger de forma reforzada a los NNA descansa en cuatro directrices. En primer lugar, la inmadurez cognitiva, la cual presume, con base científica, que esencialmente los niños y niñas poseen una capacidad limitada para comprender las implicaciones complejas y a largo plazo del tratamiento de sus datos, especialmente en lo relativo a la elaboración de perfiles y la monetización de la información. En segundo lugar, se atiende a una vulnerabilidad ontológica incrementada, puesto que, durante la etapa de desarrollo, la dependencia de los NNA es total o muy significativa, lo que reduce su capacidad de autodefensa frente a prácticas abusivas. Un tercer aspecto es la protección de su futuro, ya que los datos recolectados en la infancia pueden crean una huella digital que puede afectar profundamente la vida futura de esa persona. Finalmente, la asimetría de poder es un aspecto no menos relevante, puesto que, los NNA son particularmente susceptibles

[104] Estrada y Valenzuela (2023: 70).

[105] Comité de los Derechos del Niño (2021: 9), parágrafo 46.

[106] Comité de los Derechos del Niño (2021: 9), parágrafo 46.

a la manipulación conductual y a la influencia del marketing digital, careciendo de herramientas críticas para resistir las estrategias de captación de datos. Por ello al aceptar estos argumentos al menos es factible preguntarse si otros grupos que comparten similares características justifican también una protección reforzada. De acuerdo con trabajos previos[107], es preciso indicar que:

> …, se estima, que, aunque actualmente no se contemple una protección reforzada, ella podría articularse a partir de tres pilares: a) el trato digno que debe dispensarse a todo sujeto de derecho, pues supone respetar y morigerar su vulnerabilidad, permitiéndole ejercer el derecho de protección de datos personales en igualdad de condiciones respecto del resto de los individuos; b) el principio de licitud de los fines de los responsables de los datos personales regulado en el Artículo 3 literal a) que los obliga a hacer comprensible a sus titulares la finalidad exclusiva por la cual estos son almacenados y, en razón de ella, obtener su consentimiento y c) distintos principios y nociones que gobiernan el trato a estos colectivos vulnerables consagrados en la legislación nacional especial y/o en tratados o convenciones internacionales ratificadas por Chile[108].

IV. Personas mayores

En el contexto de las personas mayores es indudable la importancia que posee la Convención Interamericana sobre la Protección de los Derechos Humanos de las Personas Mayores ratificada por Chile (2017)[109]. Ello sin duda, establece un escenario valioso para proteger también de forma reforzada a las personas mayores, que requiriesen de dicha especial protección. No se trata de privar del ejercicio de sus derechos de manera general a quienes pertenecen a la tercera o cuarta edad en Chile sino garantizar que estos titulares puedan ejercer este derecho en plenitud.

[107] Riveros y López (2025).

[108] Riveros y López (2025:268)

[109] Arenas (2023:13); Müller (2021: 45).

V. Personas con discapacidad psíquica o intelectual

En relación con este grupo de personas también es posible observar que ellas pudiesen estar ante una situación de vulnerabilidad, la cual impidiese el pleno ejercicio de su derecho de protección de datos, con todo lo que ello implica, es decir, lo referido al tratamiento de sus distintos datos, sus derechos como titular, etc. Al igual que en el caso anterior tanto el orden internacional como el sistema jurídico interno permite discurrir respecto de la idea de una protección reforzada, puesto que, el artículo 22 de la Convención de Derechos de las Personas con Discapacidad señala, respeto de la privacidad:

> **1.** Ninguna persona con discapacidad, independientemente de cuál sea su lugar de residencia o su modalidad de convivencia, será objeto de injerencias arbitrarias o ilegales en su vida privada, familia, hogar, correspondencia o cualquier otro tipo de comunicación, o de agresiones ilícitas contra su honor y su reputación. Las personas con discapacidad tendrán derecho a ser protegidas por la ley frente a dichas injerencias o agresiones.
>
> **2.** Los Estados Partes protegerán la privacidad de la información personal y relativa a la salud y a la rehabilitación de las personas con discapacidad en igualdad de condiciones con las demás.

Asimismo, el artículo 9 de la Ley 21.331 referida al reconocimiento y protección de los derechos de las personas en la atención de salud mental establece, entre otros derechos:

> **Artículo 9.**- La persona con enfermedad mental o discapacidad psíquica o intelectual es titular de los derechos que garantiza la Constitución Política de la República. En especial, esta ley le asegura los siguientes derechos
>
> **1.** A ser reconocida siempre como sujeto de derechos.
>
> **3.** A que se vele especialmente por el respeto a su derecho a la vida privada, a la libertad de comunicación y a la libertad personal.
>
> **14.** A que su información y datos personales sean protegidos de conformidad con la ley N° 19.628.
>
> Por lo tanto, al igual que en el caso anterior, existen argumentos suficientes para poder considerar también para este grupo de personas una protección reforzada de este derecho[110].

[110] Riveros y López (2025: 271)

VI. Pacientes

La Ley 19.628 reformada en su artículo 16 bis, ya reconoce los datos de salud como una categoría especial, los datos sensibles. Con todo, esta protección se centra en la naturaleza del dato, no necesariamente en la vulnerabilidad del sujeto en el momento de la recolección de ellos. En ese sentido se debe reparar en que el paciente se encuentra en una situación de vulnerabilidad existencial. La enfermedad, el dolor o la angustia afectan la capacidad decisoria y aumentan la dependencia del sistema sanitario[111]. La asimetría de conocimiento médico y el desbalance de poder en la relación médico-paciente pueden generar que el consentimiento pueda estar viciado por el temor a no recibir tratamiento adecuado si no se aceptan las condiciones referidas al tratamiento de sus datos. Jurídicamente, entre el consentimiento informado médico y el consentimiento para el tratamiento de datos personales hay diferencias, aunque en la práctica podrían solaparse. La confusión entre ambos a menudo lleva a que el paciente crea que debe ceder sus datos para investigación o fines comerciales como condición para recibir atención médica, lo cual es naturalmente inaceptable. Por ello, destaca la noción de trato digno incorporada por la Ley 20.584 ya que ella permite reforzar los derechos de los pacientes, especialmente la privacidad, imagen[112] y la protección de datos[113].

VII. Consumidores

En la era digital, la categoría de "consumidor vulnerable" se ha expandido. Se destaca que la vulnerabilidad en mercados digitales no es solo un atributo personal, sino el resultado de la interacción entre características individuales y un entorno de mercado diseñado para explotar sesgos cognitivos. Todos los consumidores pueden ser vulnerables en ciertos contextos digitales.

---

[111] En el contexto latinoamericano es posible destacar la sentencia de la Corte Interamericana pronunciada en el caso Manuela y otros vs. El Salvador (2021) respecto del tratamiento de los datos sensibles, pues se estimó que las personas tienen derecho a que sus consultas médicas sean estrictamente confidenciales, de modo que el médico no debe infringir el secreto profesional. (Caso Manuela y otros vs. El Salvador, 2021, supra, párrs. 206 y 227; Copello (2022: 97)). Véase en tal sentido Riveros, Moraga y Arenas (En imprenta).

[112] Riveros y Arratia (2025).

[113] Riveros y López (2025: 272)

La asimetría en el mercado de datos es sustancial. El consumidor promedio desconoce qué datos se recopilan, cómo se infieren nuevos datos a partir de ellos (perfilamiento), con quién se comparten y cuál es su valor económico real[114]. Esta opacidad estructural impide naturalmente un consentimiento verdaderamente informado, lo que implica que los consumidores sufren de una vulnerabilidad estructural informativa y negociadora[115]. En este sentido, la industria emplea sistemáticamente "patrones oscuros" (*dark patterns*): interfaces de usuario diseñadas para engañar o manipular a los usuarios para que tomen decisiones que no favorecen sus intereses, como ceder más datos de los necesarios. Además, de la utilización de métodos o técnicas como el consentimiento preseleccionado, el lenguaje confuso, la ocultación de opciones de privacidad, entre otros.

En síntesis, en este acápite se permite concluir que existen argumentos jurídicos sólidos y contundentes para extender la protección reforzada de la Ley de protección de datos más allá de los niños, niñas y adolescentes. La restricción actual de la tutela especial exclusivamente a los NNA genera una inconsistencia valorativa en el ordenamiento: protege la vulnerabilidad por inmadurez o falta de capacidad, pero desatiende la vulnerabilidad por deterioro, discapacidad o asimetría estructural, dejando desprotegidos a grupos que enfrentan riesgos idénticos o superiores en el ecosistema de datos.

[114] Riefa (2022: 567)

[115] Riveros y López (2025: 272)

Capítulo 6
Derechos y obligaciones asociados al tratamiento de datos personales

Este acápite se dividirá para revisar en primer lugar lo referido a los derechos de los titulares de los datos y en una segunda parte lo relacionado con los deberes y obligaciones de los responsables en el tratamiento de los datos.

I. Derechos de los titulares

De acuerdo con el artículo 4 de la ley de protección de datos, existen diversos derechos que se le reconocen al titular de los datos, a saber, derecho de acceso, rectificación, supresión, oposición, portabilidad y bloqueo de sus datos personales. Estos derechos son, según la misma disposición legal, derechos de carácter personal, intransferibles e irrenunciables, además no pueden ser limitados por ningún acto o convención. Es indubitable que estos derechos deben ser considerados derechos de la personalidad[116]. La ley agrega un elemento interesante, pues considera que estos derechos podrán ser ejercidos por los herederos del titular de los datos salvo que el titular hubiese denegado expresamente tal derecho o la ley así lo hubiese dispuesto. En este punto se puede advertir que el considerando 27 del RPGD no aplica a la protección de datos personales de personas fallecidas, correspondiendo a los Estados miembros la competencia para establecer normas relativas al tratamiento de los datos personales de éstas[117].

[116] Contreras considera que "El otorgamiento de esta naturaleza jurídica es concordante con la tendencia internacional de conceptualizar la autodeterminación informativa y la protección de datos como un derecho fundamental". Contreras (2020: 87).

[117] A modo ejemplar el derecho español si regula la situación de quienes han fallecido y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales señala:

Artículo 3. Datos de las personas fallecidas.

1. Las personas vinculadas al fallecido por razones familiares o de hecho así como sus herederos podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión. Como excepción, las personas a las que se refiere el párrafo anterior no podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los datos de carácter patrimonial del causante.

1. Derecho de acceso

Este derecho es la puerta de entrada para ejercicio de todos los otros derechos relacionados con la protección de datos[118]. Le permite al titular de datos personales esencialmente la posibilidad de requerir al responsable que le otorgue información respecto de los datos relativos a su persona como asimismo su origen, la clase o tipo de destinatario a quienes se les informa dichos datos, el propósito o finalidad del almacenamiento, período de tiempo en que los datos son tratados, la base de licitud para ello.

> **Artículo 5º.-** Derecho de acceso. El titular de datos tiene derecho a solicitar y obtener del responsable, confirmación acerca de si los datos personales que le conciernen están siendo tratados por él, y en tal caso, acceder a dichos datos y a la siguiente información:
>
> **a)** Los datos tratados y su origen.
>
> **b)** La finalidad o finalidades del tratamiento.
>
> **c)** Las categorías, clases o tipos de destinatarios, o bien, la identidad de cada destinatario, en caso de solicitarlo así el titular, a los que se les hayan comunicado o cedido los datos o se prevea hacerlo.
>
> **d)** El período de tiempo durante el cual los datos serán tratados.
>
> **e)** Los intereses legítimos del responsable, cuando el tratamiento se base en lo dispuesto en el Artículo 13, letra d).
>
> **f)** La información significativa sobre la lógica aplicada en el caso de que el responsable realice tratamiento de datos de conformidad con el Artículo 8° bis.
>
> El responsable siempre estará obligado a entregar información y a dar acceso a los datos solicitados excepto cuando una ley disponga expresamente lo contrario.

2. Las personas o instituciones a las que el fallecido hubiese designado expresamente para ello podrán también solicitar, con arreglo a las instrucciones recibidas, el acceso a los datos personales de este y, en su caso su rectificación o supresión.
Mediante real decreto se establecerán los requisitos y condiciones para acreditar la validez y vigencia de estos mandatos e instrucciones y, en su caso, el registro de los mismos.
3. En caso de fallecimiento de menores, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada.
En caso de fallecimiento de personas con discapacidad, estas facultades también podrán ejercerse, además de por quienes señala el párrafo anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo, si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado».

[118] Pino lo califica como un derecho estratégico. Pino (2025: 54).

Respecto al modo de otorgar la información a los titulares el considerando 39 del RGPD[119] alude a un lenguaje claro y sencillo. En la ley de protección de datos no existe una norma similar. Con todo, el artículo 33 de la Ley 21.430 sobre Garantías y Protección Integral de los Derechos de la Niñez y Adolescencia en su inciso 3 señala que si el tratamiento de datos está referido a NNA la información concerniente a ellos debe expresarse en un lenguaje que les sea fácilmente comprensible. Si se consideran otro tipo de titulares como personas con discapacidad o personas mayores, la base para entregar la información de manera sencilla estaría incardinada en los tratados internacionales que protegen dichos grupos vulnerables.

2. Derecho de rectificación

Este derecho le permite al titular de los datos exigir al responsable que modifique los datos relativos a su persona cuando estos datos sean inexactos o ellos se encuentren desactualizados o incompletos.

> **Artículo 6º.-** Derecho de rectificación. El titular de datos tiene derecho a solicitar y obtener del responsable, la rectificación de los datos personales que le conciernen y que están siendo tratados por él, cuando sean inexactos, desactualizados o incompletos.
>
> Los datos rectificados deberán ser comunicados a las personas, entidades u organismos a los cuales el responsable haya comunicado o cedido los referidos datos, salvo en los casos en que dicha comunicación sea imposible o exija un esfuerzo desproporcionado.
>
> Efectuada la rectificación, no se podrán volver a tratar los datos sin rectificar.

La enmienda de los datos solicitada por el titular implica que el responsable transmita dicha rectificación, por ejemplo, en el caso en que se determine un vínculo filiativo producto de la interposición de una acción de filiación o en caso del ejercicio del derecho de cambio de nombre de acuerdo con el artículo 1 de la Ley 17.344. Pino considera que existen algunos casos en los

[119] Considerando 39 RGPD. Todo tratamiento de datos personales debe ser lícito y leal. Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados. El principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. (lo subrayado es nuestro)

cuales sería recomendable conservar los datos sin rectificar para no interferir en la comunicación con otras instituciones, señala el ejemplo del caso de cambio de nombre y sexo registral. Con todo, parece que el artículo 20 de la Ley 21.120 se sitúa bajo dicha hipótesis e instruye al Servicio de Registro Civil e Identificación informar acerca de la rectificación de la partida a más de una decena de instituciones públicas y privadas. Otro caso que el mismo autor plantea respecto de una atención de salud de emergencia, en la cual pudiese ser relevante mantener el sexo originario, sin embargo, acá se está frente a un dato sensible debido al principio de confidencialidad artículo 5 letra c) de la Ley 21.120 y al artículo 12 y 13 de la Ley 20.584 por ende prevalece este carácter, lo que hace complejo el escenario propuesto por el autor indicado[120].

3. Derecho de supresión

Este derecho consiste en la facultad de requerir la eliminación de datos de carácter personal que se pudiesen considerar innecesarios, no posean el consentimiento del interesado, han sido obtenidos o tratados de forma ilícita, o bien poseen el carácter de caducos. La fuente de la supresión puede provenir de una sentencia judicial, un acto administrativo, la ley o simplemente el titular haya ejercido su derecho de oposición y no tenga base legal para el tratamiento de los datos. Este derecho no es automático: exige una evaluación en torno a si efectivamente procede o no su cancelación. Además, la propia norma establece situaciones en la cuales no es posible conceder el derecho de supresión. A modo ejemplar la existencia de un contrato vigente entre titular y responsable o en el ejercicio de las libertades de emitir opinión y de informar.

Este derecho se relaciona con la noción de derecho al olvido que, acuerdo al artículo 17 del RGDP, se establece como un sinónimo al derecho de supresión. Ahora bien, respecto a Chile no se incorporó la misma nomenclatura. En la doctrina nacional existen coincidencia en cuanto a que el derecho de cancelación es el derecho al olvido cuando se aplica específicamente a informaciones personales que se encuentren disponibles en internet[121].

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

[120] Pino (2025: 95-96).

[121] Reusser (2021: 139). Contreras, Drago y Viollier estiman que este derecho es el derecho al olvido en sentido estricto Contreras, Drago y Viollier (2025: 93-96).

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

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

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

d) Cuando se trate de datos caducos.

e) Cuando los datos deban suprimirse para el cumplimiento de una sentencia judicial, de una resolución de la autoridad de protección de datos o de una obligación legal.

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

No procede la supresión cuando el tratamiento sea necesario:

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

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

iii. Para el cumplimiento de una función pública o para el ejercicio de una actividad de interés público.

iv. Por razones de interés público en el área de la salud pública, de conformidad con las condiciones y garantías establecidas en la ley.

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

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

4. Derecho de oposición

Este derecho permite al titular oponerse al tratamiento específico o determinado de datos frente al responsable cuando exista una razón justificada para ello. En tal sentido el legislador estima como aquellas razones relacionadas con un interés legítimo, referidas a fines de mercadotecnia o marketing directo de bienes, productos o servicios[122] o datos que se encuentren en bases públicas y que no posean otro fundamento legal para su tratamiento[123].

[122] Véase en términos similares el artículo 28 B de la Ley 19.496

[123] Contreras, Drago y Viollier lo consideran un error que se generó en el proceso legisla-

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

a) Cuando la base de licitud del tratamiento sea la satisfacción de intereses legítimos del responsable. En dicho caso podrá ejercer su derecho de oposición en cualquier momento. El responsable del tratamiento deberá dejar de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del titular, o para la formulación, el ejercicio o la defensa de reclamaciones.

b) Si el tratamiento se realiza exclusivamente con fines de mercadotecnia o marketing directo de bienes, productos o servicios, incluida la elaboración de perfiles, de conformidad con el Artículo 8° bis.

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

No procederá la oposición al tratamiento cuando éste se realice con fines de investigación científica o histórica o fines estadísticos, y siempre que fueran necesarios para el cumplimiento de una función pública o para el ejercicio de una actividad de interés público.

5. Derecho de oposición a las decisiones individuales automatizadas, incluida la elaboración de perfiles

Este derecho faculta al titular para oponerse a ser objeto de decisiones que se fundan en el tratamiento automatizado de sus datos personales[124]. Ello incluye también la elaboración de perfiles que generen efectos jurídicos o que le afectan de forma significativa. A diferencia de la norma europea ya indicada, el legislador nacional deja en términos amplios la noción de efectos que afecten significativamente a los titulares y no los vincula especialmente a los efectos jurídicos. Este derecho de oposición no puede ser ejercido cuando la decisión se requiera para ejecutar o celebrar un contrato o cuando exista consentimiento previo y expreso del titular o lo determine la ley considerando una serie de salvaguardas.

tivo de ley 21. Contreras, Drago y Viollier (2025: 93-96).

[124] Este derecho tiene como fuente el artículo 22 del RGPD, aunque la redacción de norma chilena ha mejorado los problemas suscitados por la disposición europea. Véase Garrido y Saenz (2024: 60); Contreras, Drago y Viollier, (2025:100-106).

Artículo 8° bis.- Decisiones individuales automatizadas, incluida la elaboración de perfiles. El titular de datos tiene derecho a oponerse y a no ser objeto de decisiones basadas en el tratamiento automatizado de sus datos personales, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente.

El inciso anterior no se aplicará en los siguientes casos:

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

b) Cuando exista consentimiento previo y expreso del titular en la forma prescrita en el Artículo 12.

c) Cuando lo señale la ley, en la medida en que ésta disponga el empleo de salvaguardas a los derechos y libertades del titular.

En todos los casos de decisiones basadas en el tratamiento automatizado de datos personales, inclusive aquéllos señalados en las letras a), b) y c) precedentes, el responsable deberá adoptar las medidas necesarias para asegurar los derechos y libertades del titular, su derecho a la información y transparencia, el derecho a obtener una explicación, a la intervención humana, a expresar su punto de vista y a solicitar la revisión de la decisión.

6. El derecho de bloqueo

Este derecho consiste en la posibilidad de solicitar la suspensión temporal de cualquier tipo o clase de operación de tratamiento de datos en caso de que se haya presentado una solicitud de rectificación, supresión u oposición. Esta medida es de carácter temporal y provisional y se presenta como un derecho alternativo al derecho de supresión.

Artículo 8° ter.- Derecho de bloqueo del tratamiento. 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, de conformidad con el Artículo 11 de la presente ley, mientras dicha solicitud no se resuelva.

Asimismo, el titular podrá ejercer este derecho alternativamente al de supresión en los casos del Artículo 7°.

El ejercicio de este derecho no afectará el almacenamiento de los datos por parte del responsable.

7. Derecho a la portabilidad de los datos personales

Este derecho le permite al titular pedir al responsable una copia en algún soporte electrónico, estructurado, genérico y de uso común e interoperable y para ello es menester que el tratamiento se efectué de forma autónoma y que se funde en el consentimiento del titular. La norma legal establece obligaciones para el responsable en cuanto a una serie de medidas que faciliten al titular el ejercicio de este derecho y ello conlleva la comunicación clara y precisa de la obtención de los datos, especificando las características técnicas.

> Artículo 9º.- Derecho a la portabilidad de los datos personales. El titular de datos tiene derecho a solicitar y recibir una copia de los datos personales que le conciernen, que haya facilitado al responsable, en un formato electrónico estructurado, genérico y de uso común, que permita ser operado por distintos sistemas, y a comunicarlos o transferirlos a otro responsable de datos, cuando concurran las siguientes circunstancias:
>
> **a)** El tratamiento se realice en forma automatizada, y
>
> **b)** El tratamiento esté basado en el consentimiento del titular.
>
> El responsable debe utilizar los medios más expeditos, menos onerosos y sin poner trabas u obstáculos para el ejercicio de este derecho.
>
> El responsable también debe comunicar al titular de manera clara y precisa las medidas necesarias para obtener sus datos personales y especificar las características técnicas para llevar a cabo estas operaciones.
>
> El titular tendrá derecho a que sus datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.
>
> Con todo, el ejercicio del derecho de portabilidad no supondrá la supresión de los datos ante el responsable cedente, a menos que el titular de ellos así lo pida conjuntamente en la solicitud.

Catálogo de derechos

Derecho	Artículo(s)	Contenido nuclear	Presupuestos / gatillantes	Límites / excepciones relevantes
Acceso	Art. 5º	Confirmación de tratamiento y acceso a los datos; incluye información sobre origen, finalidades, destinatarios, período de tratamiento, intereses legítimos y lógica en decisiones automatizadas.	Solicitud del titular ante el responsable; regla general de entrega salvo prohibición legal expresa.	Excepción: cuando una ley disponga expresamente lo contrario.
Rectificación	Art. 6º	Modificar o completar datos inexactos, desactualizados o incompletos; comunicación a terceros destinatarios salvo imposibilidad o esfuerzo desproporcionado.	Datos tratados por el responsable y condición de inexactitud/desactualización/incompletitud.	Tras la rectificación, no pueden volver a tratarse los datos sin rectificar.
Supresión	Art. 7º	Eliminación de datos en causales: innecesaridad, revocación de consentimiento sin otro fundamento, ilicitud, caducidad, cumplimiento de sentencia/resolución/obligación legal, u oposición exitosa.	Configuración de alguna causal del art. 7º.	No procede si es necesario para: libertad de expresión e información; obligación legal o ejecución contractual; función pública/interés público; salud pública; fines históricos/estadísticos/científicos e investigaciones de interés público; defensa/ejercicio de reclamaciones.
Oposición	Art. 8º	Oponerse a tratamiento específico/determinado en supuestos: interés legítimo; marketing directo (incl. perfiles); datos de fuente de acceso público sin otro fundamento.	Invocar causal y, en caso de interés legítimo, fundamentar brevemente la petición.	No procede cuando el tratamiento sea con fines de investigación científica/histórica o estadísticos, si es necesario para función pública o actividad de interés público.
Decisiones automatizadas y perfiles	Art. 8° bis	Derecho a oponerse y a no ser objeto de decisiones basadas exclusivamente en tratamiento automatizado (incl. perfiles) con efectos jurídicos o impacto significativo; además, salvaguardas: explicación, intervención humana, expresar punto de vista y revisión.	Decisiones automatizadas que produzcan efectos jurídicos o afecten significativamente.	No aplica si es necesaria para contrato; consentimiento previo y expreso; lo señale la ley con salvaguardas.
Bloqueo del tratamiento	Art. 8° ter + Art. 11	Suspensión temporal de operaciones de tratamiento mientras se resuelve solicitud de rectificación/supresión/oposición; alternativa a supresión en ciertos casos.	Presentación de solicitud de rectificación, supresión u oposición; petición de bloqueo mientras se resuelve.	No afecta el almacenamiento. Además, bloqueo temporal específico del art. 11 con respuesta acelerada (2 días hábiles) cuando se solicita en el procedimiento.

Portabilidad	Art. 9º	Recibir copia de datos facilitados al responsable en formato electrónico estructurado, genérico y de uso común, y comunicarlos/transferirlos a otro responsable; transmisión directa cuando sea técnicamente posible.	Tratamiento automatizado y basado en consentimiento; datos 'facilitados' por el titular.	El ejercicio no supone supresión en el responsable cedente salvo que se solicite conjuntamente.

II. Deberes y Obligaciones del responsable

1. Generalidades

El responsable de los datos o responsable es el sujeto pasivo de la relación jurídica. El concepto de responsable se encuentra definido en el artículo 2 letra n) de la ley que indica:

> **n)** Responsable de datos o responsable: 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.

Expresado, en otros términos, este sujeto determina los fines y los medios mediante los cuales son tratados los datos. La ley incluye en su enumeración toda clase de personas con independencia si son naturales o jurídicas o si tienen la categoría de pública o privada. Ella va a definir y resolver todas las decisiones atingentes al tratamiento de los datos y para ello debe establecerse un objetivo o fin determinado, es decir, se debe responder a la pregunta para qué específicamente se pretende tratar los datos.

Las obligaciones del responsable corresponden correlativamente a los derechos de los titulares de los datos. Estos deberes son de carácter general y también de carácter específico. Los primeros se encuentran contenidos en el artículo 14 de la ley en un listado no taxativo.

> **Artículo 14.-** Obligaciones del responsable de datos. El responsable de datos, sin perjuicio de las demás disposiciones previstas en esta ley,

tiene las siguientes obligaciones:

a) Informar y poner a disposición del titular los antecedentes que acrediten la licitud del tratamiento de datos que realiza. Asimismo, deberá entregar de manera expedita dicha información cuando le sea requerida.

b) Asegurar que los datos personales se recojan de fuentes de acceso lícitas con fines específicos, explícitos y lícitos, y que su tratamiento se limite al cumplimiento de estos fines.

c) Comunicar o ceder, en conformidad a las disposiciones de esta ley, información exacta, completa y actual.

d) Suprimir o anonimizar los datos personales del titular cuando fueron obtenidos para la ejecución de medidas precontractuales.

e) Cumplir con los demás deberes, principios y obligaciones que rigen el tratamiento de los datos personales previstos en esta ley.

Esta disposición referida a deberes u obligaciones generales pretende dar efectividad a los principios determinantes del tratamiento de datos. Por consiguiente, de la lectura de los numerales se puede extraer la conexión con los principios contenidos en el artículo 3.[125]

El artículo 14 inciso final además le señala una obligación específica al responsable que tenga domicilio en otro país y que efectué tratamiento de datos de personas residentes en Chile. En tal supuesto se debe indicar y mantener actualizado y operativo un correo electrónico u otro medio de carácter idóneo para que tanto titulares como la Agencia puedan comunicarse con él.

2. El deber de secreto o confidencialidad

Este deber incorporado en el artículo 14 bis de la ley, implica una obligación de carácter permanente de guardar reserva de los datos almacenados o tratados a menos que el titular los hubiere hecho manifiestamente públicos y no concluye con el término de la relación jurídica entre responsable y titular. La ley incluso considera amparados bajo este deber aquellos datos que se obtuvieron de fuentes de acceso público y en que el responsable haya efectuado alguna conducta que implique haberlos tratado. Esta obligación no impide que el responsable efectúe comunicaciones o cesiones de datos según la ley o que éste cumpla con el derecho de acceso e información al titular respecto de sus datos, ya sea que este deber sea solicitado por el titular o por

[125] Contreras, Drago y Viollier (2025:115).

un órgano público dentro de sus competencias legales. Es posible clasificar este deber como una obligación de medios, por lo tanto, el responsable debe adoptar todas las medidas necesarias para que no se incumpla con el deber de confidencialidad. Ello incluye adoptar medidas para que sus dependientes o personas naturales o jurídicas que realicen operaciones de tratamiento de datos y que estén bajo su responsabilidad también cumplan con el deber de confidencialidad.

Asimismo, esta obligación pesa sobre los organismos públicos que se encuentran bajo algún régimen especial establecido en el artículo 24 de la ley. Sin embargo, solo en relación con el requerimiento y al hecho de haber remitido dicha información.

3. El deber de información y transparencia

Este deber establecido en el artículo 14 ter de la ley le permite al titular exigirle información al responsable, la cual debe estar de forma permanente a disposición de las personas con cualquier medio accesible, para que el titular pueda ejercer sus derechos. Este deber se incardina en el principio de transparencia, ya que impone al responsable del tratamiento la obligación de poner a disposición del público información relevante respecto de sus operaciones relativas a datos personales. Esta obligación sin duda contribuye a reducir la asimetría informativa entre los titulares y los responsables. La ley establece parámetros mínimos que enmarcan esta obligación y que comprenden:

a) La política de tratamiento de datos personales que haya adoptadas por el responsable (con la inclusión de fecha y versión de la misma.

b) La singularización del responsable y su representante legal como asimismo la individualización del encargado de prevención.

c) Los medios de contacto como dirección de correo electrónico u otro medio tecnológico equivalente y accesible para la notificación de las solicitudes de los titulares.

d) Las categorías de los datos personales que se tratan, la descripción genérica del universo de individuos que incluyen sus bases de datos, las finalidades del tratamiento, la base de legitimidad del tratamiento; y en caso de tratamientos que se basan en la satisfacción de intereses legítimos, cuáles serían éstos.

e) Las medidas de seguridad adoptadas.

f) Derechos del titular para solicitar ante el responsable, acceso, rectificación, supresión, oposición y portabilidad de sus datos personales.

g) Derecho del titular de recurrir ante la Agencia, en caso de que el responsable rechace o no responda oportunamente las solicitudes que le formule.

h) La transferencia de datos personales para el caso correspondiente.

i) Plazos de conservación de los datos personales.

j) La fuente de los datos personales.

k) La existencia del derecho a la revocación retirarlo en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada.

l) Existencia de decisiones automatizadas, ello comprende la elaboración de perfiles.

Este deber claramente opera como una condición de legitimidad respecto del tratamiento de los datos personales. Así, es posible afirmar que sin la transparencia adecuada se vulnera también el principio de licitud y en definitiva el derecho de autodeterminación informativa del titular. Es por ello por lo que el artículo 14 ter es un elemento clave para asegurar el tratamiento de los datos personales en Chile bajo el marco de una transparencia eficaz.

4. El deber de protección del diseño y por defecto

Esta obligación se encuentra regulada en el artículo 14 quáter de la ley. Esta norma supone un cambio profundo en la concepción jurídica del tratamiento de datos, pues se transita de un modelo de cumplimiento formal hacia un modelo preventivo, estructural y proactivo. Este deber es una manifestación de los principios de privacidad en el diseño y privacidad por defecto establecidos en el artículo 25 RGPD.

Esta norma impone al responsable el deber de integrar a priori las medidas técnicas y organizativas necesarias destinadas a resguardar y dar cumplimiento a las disposiciones legales. Estas medidas deben tener en cuenta la naturaleza, el alcance, el contexto, los fines y los riegos asociados al tratamiento de los datos. Este deber contempla una exigencia mayor respecto al entramado técnico para que reduzca estructuralmente los riesgos inherentes al tratamiento de los datos. Este deber se sitúa frente diversas hipótesis, entre otras, una configuración deficiente de sistemas de gestión de datos o la falta de controles intermedios.

Además de la protección desde la perspectiva del diseño, esta norma también comprende la exigencia de protección por defecto y ello implica que todo tratamiento de datos debe configurarse de maneral tal que solo se traten los datos estrictamente necesarios para la finalidad especial buscada.

Por consiguiente, el responsable es obligado a la minimización de datos recolectados, a la limitación del acceso a personas estrictamente autorizadas, la restricción de divulgación indiscriminada y, finalmente, la reducción de los plazos de conservación.

Este deber incide en una amplia gama de sectores y actividades a saber; salud, educación, servicios financieros, etc. En términos generales, el diseño de los sistemas debe introducir herramientas que permitan la segmentación de acceso de acuerdo a los perfiles, registro de trazabilidad de acceso y sus modificaciones, seudonimización o anonimización según corresponda como también evaluaciones periódicas[126].

5. El deber de adoptar medidas de seguridad

Este deber está establecido en el artículo 14 quinquies de la ley y comprende la adopción de medidas de seguridad por parte del responsable del tratamiento de los datos, lo que constituye una manifestación del principio de responsabilidad y fija una estándar mínimo para la determinación o fijación de las medidas. Esta obligación de carácter específica implica considerar el estado actual de la técnica, costos, naturaleza, contexto y fines del tratamiento. Respecto de los riesgos, se debe tener en cuenta la probabilidad de que sucedan y la magnitud de sus consecuencias según la clase de datos. De acuerdo a Jijena, se configura un marco mínimo de ciberseguridad para el tratamiento de datos personales, que debe articularse con los estándares técnicos y con la Ley 21.663, denominada ley Marco de Ciberseguridad[127]. Esta ley define a la ciberseguridad en su artículo 2 Nº 6 como: "preservación de la confidencialidad e integridad de la información y de la disponibilidad y resiliencia de las redes y sistemas informáticos, con el objetivo de proteger a las personas, la sociedad, las organizaciones o las naciones de incidentes de ciberseguridad".

El deber establecido por la norma no es de carácter formal. Por el contrario, impone una adecuación permanente a la técnica y a los riesgos asociados al tratamiento, es decir, es una obligación permanente y preventiva,

[126] A modo ejemplar es posible señalar que la Ley 20.584 modificada por la Ley 21.541 referida a las atenciones mediante telemedicina regula aspectos técnicos y operativos referidos a esta materia.
"Artículo 10 bis.- Las plataformas tecnológicas empleadas en las acciones y prestaciones de salud digital, así como las que almacenan y tratan datos personales deberán estar acreditadas en cuanto al cumplimiento de las normas y estándares técnicos que establezca el Ministerio de Salud a través de un reglamento y las normas técnicas respectivas"

[127] Jijena (2025: 203).

que pretende evitar la destrucción o la pérdida de datos, ya sea de forma accidental o culpablemente. El legislador fija para este propósito un listado no taxativo de medidas técnicas y organizativas:

a) La seudonimización y el cifrado de datos personales.

b) La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

c) La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.

d) Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Finalmente, el artículo 14 quinquies modifica la carga de la prueba, ya que si acontece un incidente de seguridad para efectos de controversia judicial o administrativa, le corresponde al responsable acreditar tanto la existencia como asimismo el funcionamiento de las medidas de seguridad, que hayan sido adoptadas previamente en consideración a los niveles de riesgo y a la tecnología disponible.

6. El deber de reportar vulneraciones

El artículo 14 sexies establece el deber de reportar a la Agencia de Protección de Datos las vulneraciones de las medidas de seguridad, es decir, incidentes que involucren u ocasionen riesgos razonables a derechos y libertades de los titulares, mediante alteración, filtración, pérdida o incluso destrucción de datos o comunicación no autorizada de dichos datos[128]. El responsable no solo debe comunicar o reportar las vulneraciones, es decir, no es solo una actuación de índole formal, sino que la ley le exige describir la naturaleza de las vulneraciones, sus consecuencias, cuáles categorías de datos fueron transgredidas, el número aproximado de afectados, como, asimismo, qué medidas se adoptaron para gestionar las vulneraciones y precaver nuevos incidentes. La ley no fija ni la forma ni el plazo para comunicar las vulneraciones a la Agencia, solo señala que debe efectuarse por medios más expeditos posibles y sin dilaciones indebidas.

[128] Se muestran críticos frente a la exigencia del legislador de establecer "la existencia de un riesgo razonable para los derechos y titulares de los titulares" Garrido y Saenz (2024: 75).

Asimismo, surge una especial obligación para el responsable de informar a los titulares o sus representantes en el caso de que los incidentes afecten a datos personales sensibles, datos relativos a niños y niñas menores de catorce años o datos relativos a obligaciones de carácter económico, financiero, bancario o comercial. Esta notificación debe efectuarse a cada afectado, a menos que ello no fuese posible. En dicha situación, deberá difundirse por un medio masivo de alcance nacional. Además, se adiciona a esta obligación que la comunicación debe efectuarse en un lenguaje comprensible, que debe incluir los datos afectados, los posibles efectos y las medidas adoptadas para solucionar las vulneraciones.

Capitulo 7
Acciones judiciales vinculadas a datos personales

La Ley 21.719 configura un nuevo modelo de tutela judicial del derecho a la protección de los datos personales, superando el enfoque predominantemente declarativo y fragmentario de la normativa anterior. En este marco, las acciones judiciales vinculadas a datos personales se erigen como instrumentos esenciales para la efectividad del derecho fundamental a la autodeterminación informativa, entendido como la facultad del titular de controlar el tratamiento de la información que le concierne.[129]

Desde una perspectiva judicial, estas acciones no cumplen únicamente una función reparadora, sino también preventiva, correctiva y estructural, orientada a restablecer la legalidad del tratamiento y a reequilibrar la asimetría informativa entre titulares y responsables.[130]

Hablar de "acciones judiciales vinculadas a datos personales" exige distinguir: (i) mecanismos judiciales creados por la propia Ley 21.719 (en particular, el reclamo de ilegalidad contra actos de la Agencia y la acción indemnizatoria); (ii) acciones constitucionales y legales generales que históricamente han cumplido una función sustitutiva o complementaria (recurso de protección, responsabilidad civil común, acciones colectivas en consumo, entre otras); y (iii) remedios administrativos que, aun siendo extrajudiciales, condicionan el acceso al juez o determinan el contenido del litigio posterior.

Así las cosas, se adopta un modelo mixto de tutela, en el que la Agencia actúa como órgano especializado de supervisión y sanción, sin excluir el acceso a los tribunales de justicia. Este diseño responde a una lógica de subsidiariedad relativa, que no subordina rígidamente la tutela judicial a la previa actuación administrativa, especialmente cuando se encuentran comprometidos derechos fundamentales o cuando la tutela administrativa resulta insuficiente o tardía.[131] Para la judicatura, este modelo implica reconocer que la acción judicial en materia de datos personales no es excepcional, sino un componente estructural del sistema de protección.[132]

[129] Rodotà (2003: 63–70; 83-90).

[130] Bygrave (2002, 96–103).

[131] Lynskey (2015:189–194).

[132] De Hert y Gutwirth (2006: 61–67).

Para este acápite se adopta una aproximación funcional-comparada: se analizan los fines que cumplen los remedios (cesación, corrección, sanción, reparación) y su asignación institucional, contrastando el diseño chileno con el RGPD (artículos. 77 a 79 y 82) y con la LGPD brasileña (responsabilidad civil y sanciones administrativas). El objetivo no es trasplantar modelos, sino evaluar la coherencia del sistema chileno con principios de tutela judicial efectiva, proporcionalidad y debido proceso.

I. Racionalidad del nuevo modelo de tutela

La reforma se sitúa en el cruce entre constitucionalismo de derechos y regulación económica. Por una parte, la protección de datos se entiende como una proyección del derecho a la vida privada (artículo 19 N° 4 CPR) y, en contextos determinados, como garantía frente a prácticas discriminatorias, extractivas o de vigilancia. Por otra, se trata de una regulación del poder informacional: fija condiciones de licitud del tratamiento, distribuye cargas de prueba ("*accountability*") y crea incentivos de cumplimiento mediante sanciones y publicidad de infractores.[133]

Bajo el régimen previo, la tutela se caracterizó por un *enforcement* débil: los derechos existían, pero el titular debía internalizar costos de litigación y prueba, las sanciones administrativas eran inexistentes y la interpretación se fragmentaba entre tribunales.[134] La Ley 21.719 responde con un modelo de autoridad de control: la Agencia instruye procedimientos, dicta resoluciones fundadas, puede imponer multas y medidas correctivas, y administra un Registro Nacional de Sanciones y Cumplimiento público por cinco años. Este giro explica que las "acciones judiciales" centrales ya no se dirijan directamente contra el responsable, sino que primero se deriven a la gestión de la Agencia.

En términos de teoría del derecho administrativo sancionador, la Agencia asume un rol mixto: regulador técnico, fiscalizador y órgano sancionador. La judicialización se reubica en un control ex post que debe equilibrar deferencia técnica y protección de garantías: publicidad, motivación, contradictoriedad, prueba y proporcionalidad de la sanción. De ahí que el diseño procesal del

[133] Rodotà (2003: 37–44 y 63–70); Bygrave (2002: 6–12 y 87–93); Lynskey (2015: 21–27 y 178–183) ; De Hert y Papakonstantinou (2016: 626–631); Bennett y Raab (2006: 95–102).
134 Ayres y Braithwaite (1992:19–25 y 101–105).; OECD (2014: 23–29).

reclamo de ilegalidad y la regla de acceso a la indemnización se vuelvan piezas dogmáticas claves.[135]

II. Tutela administrativa ante la Agencia

El primer nivel de tutela es privado y obligatorio en la práctica: los derechos se ejercen ante el responsable de datos. La ley exige que los responsables implementen mecanismos tecnológicos sencillos y disponibles, y consagra gratuidad como regla (con excepciones acotadas en acceso y portabilidad). Esta etapa cumple una función de eficiencia: si el conflicto se resuelve aquí, se evita la intervención de la Agencia y del juez, reduciendo costos de transacción y cargas institucionales.

El segundo nivel es el procedimiento administrativo de tutela de derechos del artículo 41 (Ley 21.719). El titular puede reclamar ante la Agencia cuando el responsable deniega una solicitud o no responde dentro de plazo. El reclamo debe presentarse por escrito (físico o electrónico) dentro de treinta días hábiles desde la respuesta negativa o desde el vencimiento del plazo de respuesta. La Agencia controla admisibilidad y, si acoge a tramitación, confiere traslado al responsable (treinta días corridos, prorrogables por igual plazo). Solo si existen hechos sustanciales, pertinentes y controvertidos puede abrirse un término probatorio de diez días hábiles. La resolución debe ser fundada y el procedimiento no puede exceder seis meses.

Un elemento de especial relevancia práctica es la cautelar administrativa: al interponer el reclamo, y a petición fundada del titular, la Agencia puede suspender el tratamiento de los datos objeto del conflicto, previa audiencia del responsable, y en casos justificados. Funcionalmente, esta medida opera como una tutela anticipada de cesación. En protección de datos, la demora puede ser irreversible (difusión, perfilamiento, decisiones automatizadas), por lo que la existencia de una cautelar específica es un avance significativo.

En paralelo, el artículo 42 regula el procedimiento administrativo sancionatorio por infracción de ley. La Agencia puede iniciarlo de oficio o a petición de parte, incluso como consecuencia de una reclamación de tutela. La estructura contiene formulación de cargos, descargos, término probatorio eventual, apreciación por sana crítica y resolución final fundada. La ley clasifica infracciones en leves, graves y gravísimas y prevé sanciones principales

[135] Black (2002: 1–10); OECD (2015:15–22 y 73–77); **Sunstein** (1990: **38–44 y 90–96**).

(amonestación y multas) y accesorias (como suspensión de actividades de tratamiento en supuestos acotados). Desde la óptica de acciones judiciales, el punto decisivo es que la resolución sancionatoria también se somete al control judicial del artículo 43.

El doble carril (tutela y sanción) exige coordinación. Una misma conducta puede, a la vez, vulnerar un derecho del titular y constituir infracción sancionable. La interpretación deberá evitar incoherencias: por ejemplo, una decisión de tutela que ordene rectificación, y otra sancionatoria que relativice la ilicitud. Un enfoque institucionalmente adecuado es tratar el expediente de tutela como fuente de antecedentes para la sanción, preservando contradicción y defensa y, distinguiendo objeto: la tutela se orienta a corregir y restituir derechos; la sanción, a disuadir y reprochar.[136]

III. Acciones judiciales contra la Agencia: reclamo de ilegalidad

El artículo 43 establece el procedimiento de reclamación judicial ("reclamo de ilegalidad") contra actos de la Agencia. Procede cuando el interesado estime ilegal un acto que paraliza el procedimiento o una resolución final o de término. La competencia corresponde a la Corte de Apelaciones de Santiago o la del domicilio del reclamante, a elección de este último. En materia de tutela de derechos, el artículo 41 dispone expresamente que la resolución que declara inadmisible un reclamo y la que lo resuelve pueden impugnarse por esta vía dentro de quince días hábiles desde su notificación.[137]

El reclamo exige precisión: individualizar el acto, indicar normas infringidas, explicar la forma de infracción y el agravio. La Corte puede declarar inadmisible por incumplimiento formal y puede dictar orden de no innovar ante riesgo de daño irreparable. En datos personales, la orden de no innovar puede ser central para detener tratamientos que generen exposición pública, perfilamiento o decisiones automatizadas de alto impacto.[138]

El procedimiento combina elementos de control de legalidad con espacios de cognición. La Corte solicita informe a la Agencia (diez días) y puede abrir término de prueba, regido por reglas para los incidentes del Código de

[136] Huergo (2007:89–97 y 181–186); Nieto (2012: 203–210).
[137] Bermúdez (2018: 455–463).
[138] Cassagne (2011: 417–423); Cordero (2019: 169–173).

Procedimiento Civil. Si acoge el reclamo, ordena la rectificación del acto y la dictación de la resolución que corresponda. Tratándose de reclamaciones contra resoluciones sancionatorias, puede confirmar o revocar, establecer o desechar la infracción y mantener, dejar sin efecto o modificar la sanción. Esto permite un control de proporcionalidad y razonabilidad de la respuesta sancionatoria, no solo un examen formal.[139]

En clave dogmática, el desafío será calibrar la intensidad del control judicial sobre decisiones técnicamente densas (seguridad, anonimización, transferencia internacional, etc.). Un estándar plausible es el control de legalidad reforzada: revisión de competencia, procedimiento, motivación y proporcionalidad, con deferencia limitada respecto de apreciaciones técnicas, salvo error manifiesto o falta de fundamentación. La motivación y la calidad del expediente serán, por tanto, determinantes para la estabilidad de las decisiones de la Agencia.[140]

IV. Acción indemnizatoria y problemas de diseño

La responsabilidad civil es regulada expresamente en el artículo 47. El responsable debe indemnizar el daño patrimonial y extrapatrimonial que cause al titular cuando infrinja principios, derechos u obligaciones del régimen y de ello derive perjuicio. El reconocimiento del daño extrapatrimonial es estructural: permite captar lesiones típicas del mundo digital (pérdida de control, angustia, estigmatización, discriminación), que no siempre se traducen en daño material inmediato.[141]

La ley adopta, sin embargo, una regla de acceso condicionada: la acción indemnizatoria puede interponerse una vez ejecutoriada la resolución que haya acogido favorablemente el reclamo del titular ante la Agencia, o una vez firme la sentencia dictada en el reclamo de ilegalidad si éste se interpuso. Además, la acción se tramita por procedimiento sumario. Funcionalmente, se busca evitar duplicidad: la constatación de la infracción se concentra en sede administrativa (y su control en el artículo 43), y el juez civil se focaliza en daño, causalidad y cuantificación.[142]

[139] Vergara (2016: 391–397).

[140] Esteve (2009: 117–123).

[141] Bygrave (2002: 155–160); Rodotà (2003: 93–98); González (2014: 186–191); Floridi (2013: 141–145); Lynskey (2015: 178–183); Doneda (2006:121– 126).

[142] Sunstein (1990: 90–96); Mashaw (1983: 23–31 y 241–245); OECD (2014: 29-34); Black (2002: 6–9); Cassagne (2011: 417–423).

Esta arquitectura tiene virtudes y riesgos. Entre las virtudes, promueve la uniformidad interpretativa (la Agencia fija estándares y la Corte controla legalidad), reduce litigios repetidos sobre la ilicitud y puede disminuir asimetrías de información mediante el expediente administrativo. Entre los riesgos, puede tensionar la tutela judicial efectiva si la vía administrativa se vuelve lenta o inaccesible. En un escenario de saturación de la Agencia, la exigencia de ejecutoria podría transformar la reparación en una promesa tardía. Una lectura conforme a la Constitución y a estándares interamericanos debería, al menos, asegurar que la impugnación por inactividad o demora sea realmente eficaz.[143]

Un aspecto dogmático adicional es la distribución de la carga de la prueba en la cadena administrativa-judicial. La ley atribuye al responsable el deber de acreditar la licitud del tratamiento y, en general, impone obligaciones de información y trazabilidad. Esto debe proyectarse en el juicio civil: una vez constatada la infracción, el responsable difícilmente podrá alegar ignorancia técnica sobre su propio tratamiento. En términos probatorios, la documentación de cumplimiento (políticas, registros, evaluaciones de riesgo, medidas de seguridad, respuestas a solicitudes del titular) funcionará como prueba central, y su ausencia puede operar como indicio grave en la construcción de causalidad y cuantía del daño.[144]

En materia de prescripción, el artículo 47 fija cinco años desde la ejecutoria de la resolución administrativa o sentencia judicial que imponga la multa respectiva. La referencia a la multa sugiere un anclaje en el procedimiento sancionatorio; ello plantea interrogantes cuando la tutela concluye con órdenes correctivas sin multa. En ausencia de jurisprudencia, una interpretación sistemática razonable es extender el *dies a quo* a la ejecutoria de la resolución de tutela que establezca la infracción y ordene medidas, aunque no imponga multa, para no dejar sin régimen temporal a la reparación.[145]

Comparativamente, el RGPD reconoce derecho a indemnización por daños materiales e inmateriales (artículo 82) y permite acciones judiciales directas contra responsables (artículo 79) "sin perjuicio" de reclamaciones ante la autoridad. La opción chilena es más restrictiva en acceso inmediato, pero puede ganar en coherencia y economía procesal si la Agencia funciona

[143] Mashaw (1983: 23-31); Cappelletti y Garth (1978: 67–73 y 95–99); Corte Interamericana de Derechos Humanos, Caso Baena Ricardo y otros vs. Panamá, 2 de febrero de 2001, párrs. 124–129.

[144] De Hert y Papakonstantinou (2016: 626–633); Kuner (2007: 69–73); Working Party (WP29) (2010: 9–12); Taruffo (2005: 131–137); De Ángel (1993: 57–63).

[145] García de Enterría y Fernández (2011: 205–209); Larenz (2001: 316–322); Fix-Zamudio (2005: 423-430); Corte Interamericana de Derechos Humanos, Caso Cantos vs. Argentina, 28 de noviembre de 2002, párrs. 52–55.

con eficacia. La experiencia brasileña bajo la LGPD, donde coexisten responsabilidad civil (artículo. 42) y sanciones administrativas, muestra que la litigación puede aumentar significativamente ante brechas masivas; el filtro administrativo chileno busca amortiguar ese efecto, aunque al costo de introducir otra eventual salida/atochamiento.[146]

V. Convivencia con acciones generales

El régimen reformado no elimina las acciones constitucionales. El recurso de protección (artículo 20 CPR) ha sido utilizado para controvertir tratamientos de datos bajo la óptica de vida privada, honra, igualdad y otros derechos. Tras la entrada en vigor de la Ley 21.719, es probable que persista su uso, especialmente en casos de urgencia o de incertidumbre interpretativa. La pregunta será de coordinación: si el sistema especial ofrece un remedio idóneo y expedito, los tribunales podrían preferir la vía especializada; si no lo ofrece, el recurso seguirá cumpliendo un rol supletivo de urgencia.[147]

En daños masivos, la interacción con el derecho del consumidor puede ser decisiva. Brechas de seguridad en empresas con grandes bases de clientes pueden activar simultáneamente la competencia de la Agencia (por infracción a obligaciones de seguridad y transparencia) y mecanismos colectivos del estatuto de consumo. Aquí se abre un debate de *ne bis in idem* y de distribución de competencias, que deberá resolverse con criterios de identidad de hecho y fundamento jurídico, y con coordinación interinstitucional.[148]

Respecto de órganos públicos, la Ley 21.719 configura responsabilidad administrativa del jefe superior del servicio, con multas calculadas como porcentaje de remuneración y posibles suspensiones en casos relevantes, además de la intervención de Contraloría para investigaciones de responsabilidad funcionaria. Las resoluciones de la Agencia también se controlan por reclamo de ilegalidad. Este diseño enfatiza *accountability* personal en la cúspide administrativa, pero puede enfrentar dificultades prácticas (prueba

[146] Reglamento (UE) 2016/679 (RGPD), artículo 82 ("Derecho a indemnización y responsabilidad"); Reglamento (UE) 2016/679 (RGPD), artículo 79 ("Derecho a la tutela judicial efectiva contra un responsable o encargado"), ap. 1 ("*Without prejudice…*"); Brasil, *Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), Seção III ("Responsabilidade e Ressarcimento de Danos")*, artículo 42.

[147] Nogueira (2010: 145-151).

[148] Ley 19.496 (LPDC), régimen de acciones (incluye acciones colectivas y legitimación del SERNAC/ asociaciones / grupo de consumidores).

de imputación, cultura organizacional, recursos tecnológicos) y deberá ser compatible con principios del derecho disciplinario.[149]

VI. Perspectiva comparada: RGPD y LGPD

La comparación funcional ayuda a evaluar si el sistema chileno ofrece un conjunto completo de remedios: cesación/corrección, sanción y reparación. En la Unión Europea, el RGPD estructura la tutela como un "triángulo": queja ante autoridad (artículo 77), remedio judicial contra la autoridad por decisión o inactividad (artículo78) y acción judicial directa contra responsable/encargado (artículo79), además de indemnización (artículo 82). La premisa es la multiplicidad de puertas, con especial énfasis en el derecho a un recurso judicial efectivo.

El modelo chileno converge con el derecho europeo en la centralidad de la autoridad administrativa especializada y en el control judicial de sus actos, materializado en el reclamo de ilegalidad como vía de revisión jurisdiccional. No obstante, se aparta del diseño del Reglamento General de Protección de Datos al condicionar el acceso a la acción indemnizatoria a la existencia de un pronunciamiento administrativo o judicial previo que haya quedado firme y ejecutoriado.[150]

Esta opción normativa puede comprenderse como una apuesta por la coherencia sistémica del *enforcement*: en una primera fase, la ilicitud del tratamiento se determina en sede técnica, bajo estándares uniformes y sujeta a control judicial; en una segunda fase, ya despejado el debate sobre la infracción, el proceso civil se concentra en la reparación del daño. El diseño busca así evitar decisiones contradictorias, reducir litigios redundantes y aprovechar la especialización técnica de la Agencia.

Con todo, la eficacia de este modelo depende de un supuesto empírico-institucional decisivo: la capacidad de la Agencia para resolver con oportunidad, calidad técnica y recursos suficientes. Si dicha condición se satisface, el filtro administrativo puede incrementar la eficiencia y racionalidad del sistema de tutela. Si, por el contrario, la Agencia enfrenta retrasos estructurales o déficits operativos, la exigencia de un pronunciamiento previo ejecutoriado corre el riesgo de debilitar el acceso efectivo a la reparación, transformando

[149] Cordero (2019: 73–79 y 161–167).

[150] Fix-Zamudio (2005: 423–430).

el derecho a indemnización en una expectativa diferida y potencialmente ilusoria.[151]

En Brasil, la LGPD contempla responsabilidad civil por daños patrimoniales y morales, individuales o colectivos (artículo 42), y un régimen sancionatorio aplicado por la *Autoridade Nacional de Proteção de Dados* (ANPD). La práctica ha mostrado una intensa litigación, especialmente por incidentes de seguridad. El caso brasileño es útil como advertencia: sin criterios robustos de prueba y cuantificación, la judicialización puede producir decisiones divergentes y costos reputacionales desproporcionados. El expediente administrativo puede funcionar como un mecanismo de estandarización probatoria; en Chile, esa estandarización es más fuerte por el requisito de ejecutoria previa.[152]

VII. Desafíos interpretativos

El régimen chileno plantea problemas dogmáticos que, por su novedad, requerirán construcción jurisprudencial y doctrinal desde el 1 de diciembre 2026.

El de primero de ellos se refiere a la relación entre agotamiento administrativo y tutela judicial efectiva. El filtro del artículo 47 debe leerse a la luz de garantías de debido proceso y acceso a la justicia: si la vía administrativa se torna ineficaz, los tribunales podrían verse presionados a habilitar remedios constitucionales o interpretaciones correctivas (por ejemplo, controlar inactividad mediante el propio artículo 43 o por vías generales).

En segundo lugar, se encuentra el alcance vinculante del expediente administrativo en el juicio civil. Un diseño eficiente debiera reconocer que la infracción establecida por resolución ejecutoriada no se reabre, limitando el debate civil a daño y causalidad, salvo vicios graves del procedimiento administrativo. De lo contrario, se neutraliza la economía procesal buscada por el legislador.

En tercer lugar, nos encontramos con la problemática del estándar y la cuantificación del daño extrapatrimonial. La reparación debe evitar tanto el

[151] Ayres y Braithwaite (1992:101–105 y 120–123).

[152] Brasil, *Lei n.º 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), artículo 42, Seção III ("Da Responsabilidade e do Ressarcimento de Danos")*, artículo 52-54; Doneda y Mendes (2014: 213–220); Mendes (2020: 287–295); Bioni (2019:351-357).

automatismo (daño moral *per se* por cualquier infracción) como la exigencia probatoria imposible. Criterios como la naturaleza del dato, el alcance de la difusión, la duración del tratamiento, el número de afectados y la conducta del responsable (diligencia, mitigación, cooperación) permiten objetivar la evaluación.

En cuarto lugar, se encuentra la función de las medidas cautelares (suspensión del tratamiento y orden de no innovar). En datos, el tiempo es un factor constitutivo del daño; por ello, los estándares de procedencia y los umbrales de riesgo deben construirse con sensibilidad a la irreversibilidad. El control judicial de estas medidas será clave para mantener la proporcionalidad sin vaciar de contenido la tutela.

En quinto lugar, se encuentra la coordinación entre de la agencia y determinadas autoridades sectoriales, particularmente en incidentes de seguridad masivos y en ámbitos regulados (como en salud o financiero). La solución institucional más estable es una práctica administrativa consistente y acuerdos de coordinación que reduzcan el riesgo de duplicidad sancionatoria y definan prioridades de investigación.

Finalmente, se encuentra la problemática relativa a la legitimación y representación de titulares vulnerables (NNA) y la tutela de datos sensibles. La ley califica como infracciones gravísimas ciertos tratamientos de datos de NNA y datos sensibles, lo que anticipa un estándar más estricto de diligencia. En litigios posteriores, el juez deberá ponderar cómo estos factores inciden en el daño y en medidas de mitigación, y si corresponde elevar el umbral de protección cautelar. La comparación con la práctica europea muestra que, en contextos de alta vulnerabilidad, la proporcionalidad se interpreta a favor de medidas más intensas de cesación y de mayores estándares de transparencia.

Capitulo 8
Responsabilidad civil de la infracción al derecho de datos personales

I. Consideraciones generales

Son variados los derechos de la personalidad que se ven incardinados en el tratamiento de datos personales. Desde luego, se encuentra el derecho a la protección de datos personales o audeterminación informativa (así como las facultades que este comprende). Se encuentran también los denominados derechos ARCO (rectificación, cancelación y oposición al tratamiento de datos)[153], así como el derecho a la identidad digital, a la propia imagen, a la honra, al honor o a la privacidad. Estos derechos pueden verse lesionados con la actuación del responsable de datos, lo que amerita una nítida distinción en torno al objeto de protección a que cada uno de ellos apunta, lo que determinará el esquema de responsabilidad civil aplicable para el resarcimiento de los daños provocados al titular de los datos.

En tal sentido, si entendemos el derecho a la protección de datos personales como la facultad de autocontrol que un titular tiene sobre su información personal, el resarcimiento de los perjuicios derivados por esa falta de control es la esfera correspondiente a su tutela, en tanto que los daños derivados, por ejemplo, de la difusión de aspectos íntimos de la persona o de la publicación de su imagen sin mediar su consentimiento incidirán en su derecho a la intimidad, vida privada o propia imagen, respectivamente.

Situando a la persona, su dignidad inherente y el libre desarrollo de su personalidad como centro de la regulación jurídica, desplegar la tutela frente a todo daño que se le irrogue es central, la que desde el punto de vista del derecho civil se traduce, en general, en el resarcimiento de los perjuicios guiado por el principio de reparación integral del daño vigente en el ámbito de la responsabilidad civil extracontractual[154].

[153] Contreras, Drago y Viollier (2024: 3).

[154] Corral (2004: 271); Egusquiza (2025: 215).

Esta óptica permite vislumbrar casos en que de una misma conducta pueden derivar daños a más de un bien jurídico[155], todos los cuales deben ser reparados por medio de las reglas de responsabilidad civil que resulten aplicables en el esquema determinado por la ley, sea mediante el régimen especial, que atiende al derecho a la protección de datos personales, sea a través del sistema general de la responsabilidad civil aquiliana, conforme las reglas del código civil, tratándose de otro derecho de la personalidad[156]. En este sentido, la normativa vigente en la Unión Europea ha señalado en el considerando 146 del RGPD que el régimen que prevé para la compensación de los daños derivados de un tratamiento de datos personales en infracción de la normativa ha de entenderse "sin perjuicio de cualquier reclamación por daños y perjuicios derivada de la vulneración de otras normas del Derecho de la Unión o de los Estados miembros", de lo que se desprende el carácter acumulable de la acción por responsabilidad civil por daños al derecho a la protección de datos personales que establece en su artículo 82 con la acción indemnizatoria en materia de protección civil del derecho al honor, a la intimidad o a la propia imagen[157].

Aun cuando el enfoque tecnológico neutro es el que se impone, con lo que resulta indiferente el soporte en que la información se contenga y la forma que esta revista[158], preciso es considerar el impacto que las nuevas tecnologías de la información han tenido en el tratamiento generalizado de datos personales lo que, en el ámbito jurídico, ha sido enfrentado contemplando una serie de reglas y garantías[159].

Dedicaremos las próximas líneas a revisar el régimen de responsabilidad civil propio establecido para los daños provocados al derecho a la protección de datos personales, en el que la regulación nacional ha seguido de cerca el modelo adoptado por el RGDP.

El RGDP "ofrece una respuesta preventiva y sancionatoria frente a conductas irresponsables o tratamientos ilícitos de los datos personales"[160], introduciendo mecanismos ante autoridades competentes de los Estados a fin de controlar de manera efectiva y supervisar las responsabilidades de los operadores, las que se complementan con mecanismos jurídico-privados de tutela civil, entre las que destaca el sistema de responsabilidad civil establecido en su artículo 82.

El artículo 82 del Reglamento 2016/679, en lo pertinente dispone:

---

[155] Rubí (2018: 54).

[156] Riveros y López (2025: 274)

[157] Rubí (2019: 214).

[158] Contreras, Drago y Viollier (2024: 25).

[159] Biblioteca del Congreso Nacional (2024:177).

[160] Cavaller (2024: 255).

> Derecho a indemnización y responsabilidad 1.Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos.
>
> 2.Cualquier responsable que participe en la operación de tratamiento responderá de los daños y perjuicios causados en caso de que dicha operación no cumpla lo dispuesto por el presente Reglamento. Un encargado únicamente responderá de los daños y perjuicios causados por el tratamiento cuando no haya cumplido con las obligaciones del presente Reglamento dirigidas específicamente a los encargados o haya actuado al margen o en contra de las instrucciones legales del responsable.
>
> 3.El responsable o encargado del tratamiento estará exento de responsabilidad en virtud del apartado 2 si demuestra que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios [...].

El RGPD engloba el tratamiento automatizado de datos, total o parcialmente, y el no automatizado, no obstante, tiene en consideración el ámbito virtual en que se mueven los datos personales profusamente en la actualidad, teniendo como eje central el consentimiento inequívoco, expreso y revocable de las personas, el que se articula mediante condiciones de validez formales y transparentes, ofreciendo a los titulares de la información herramientas para defender sus derechos, generando las correspondientes responsabilidades a aquellos que infrinjan el correcto tratamiento, mecanismo que se incardina con la finalidad de la responsabilidad civil, entendida como la facultad de rendición de cuentas por las infracciones de la normativa y la asunción por parte del responsable de las consecuencias perjudiciales que se deriven de estas[161].

El sistema de responsabilidad civil adoptado por el Reglamento gira en torno al principio de responsabilidad proactiva, también denominado *accountability*, asumiendo que el tratamiento de datos personales puede ser una fuente de riesgos , imponiendo a los agentes del tratamiento de datos la necesidad de evaluar esos riesgos y adoptar las medidas técnicas y organizativas demostrables ante el titular de la información y ante el órgano de supervisión, con objeto de prevenir y minimizar los riesgos detectados

[161] Cavaller (2024: 258).

procurando con ello evitar daños a las personas[162]. La estructura de la disposición en comento precisa que el órgano jurisdiccional determine los elementos relativos a la prueba del daño sufrido y la cuantificación de la indemnización.

Siguiendo el desarrollo de la jurisprudencia del Tribunal de Luxemburgo[163], la doctrina califica el sistema de responsabilidad civil establecido como un mecanismo de responsabilidad por culpa con inversión de la carga de la prueba, pues es el responsable del tratamiento de datos a quien corresponde demostrar que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios[164]. Así, únicamente en el supuesto que el sujeto responsable pueda acreditar que ha implementado con una diligencia razonable todas las medidas técnicamente adecuadas podrá exonerarse de la responsabilidad impuesta por el artículo 82. En este sentido se ha pronunciado el TSE en sentencia 188/2022 de 15 de febrero al señalar en su fundamento de derecho tercero: "No basta con diseñar los medios técnicos y organizativos necesarios, también es necesaria su correcta implantación y su utilización de forma apropiada, de modo que también responderá por la falta de diligencia en su utilización, entendida como una diligencia razonable atendiendo a las circunstancias del caso".

Sin embargo, es necesario tener presente que la sola infracción de principios y derechos no constituye por sí misma elemento suficiente para reclamar una indemnización de perjuicios, se requiere la existencia real y efectiva del daño y una relación de causalidad entre los daños y la infracción. Al decir de la doctrina "la aportación en el proceso civil de una resolución administrativa firme que constate una infracción en materia de protección de daños no ha de equivaler en forma necesaria a una declaración de responsabilidad civil"[165]. En este sentido se ha pronunciado el TSE en sentencia 1495/2024 de 19 de marzo, señalando en el número 5 de su fundamento de derecho tercero:

> No puede considerarse que toda infracción de las disposiciones sobre protección de datos personales dé lugar, por sí sola, a un derecho a una indemnización a favor del interesado. Por el contrario, para la pertinencia de la indemnización deberían concurrir tres requisitos cumulativos: (i) un tratamiento de datos personales en infracción de las disposiciones legales pertinentes; (ii) la existencia de daños y perjuicios para el interesado; y (iii) una relación de causalidad entre

[162] Cavaller (2024: 263).

[163] Tribunal de Justicia de la Unión Europea, sala tercera, sentencia de 21 de diciembre de 2023, *Krankenversicherung Nordrhein*, C-667-21, EU:2023:1022, apartado 103.

[164] Cavaller (2024: 265).

[165] Rubí (2019: 219).

dicho tratamiento ilícito y esos daños y perjuicios.

En igual sentido, la STJU de 14 de diciembre de 2023, asunto C 456/22, declara que es preciso que el afectado pruebe que la vulneración de la normativa de protección de datos le haya causado algún perjuicio, por mínimo que sea, y que "El interesado debe demostrar que las consecuencias de esa infracción que afirma haber sufrido constituyen un perjuicio distinto de la mera infracción de las disposiciones de dicho Reglamento".

En este caso únicamente concurre el primero de los requisitos indicados que, por sí solo, es insuficiente a los efectos pretendidos por los demandantes. Como resalta la primera STJUE antes citada, "la realización de daños y perjuicios en el marco de tal tratamiento solo es potencial; [...] la infracción del RGPD no conlleva necesariamente daños y perjuicios, y [...] debe existir una relación de causalidad entre la infracción en cuestión y los daños y perjuicios sufridos por el interesado para fundamentar un derecho a indemnización". Por lo que insiste en que una cosa es la infracción de la normativa sobre protección de datos, que puede dar lugar a una sanción administrativa y otra la obtención de una indemnización que no puede ser automática; sin que quepa una equiparación lineal entre infracción e indemnización.

De otra parte, en materia de responsabilidad civil por daños se ha de tener presente que "la acreditación de cumplimiento de las normas que establecen deberes de cuidado no excluye, por sí sola, la apreciación de culpa y, en efecto, la responsabilidad del demandado"[166].

En consecuencia, para hacer nacer la responsabilidad civil para la indemnización de los perjuicios causados al derecho a la protección de datos personales, el titular afectado deberá probar la condición de responsable del tratamiento de datos personales; una infracción de la normativa sobre protección de datos; los daños sufridos; y, la relación de causalidad entre la infracción y el resultado dañoso[167].

[166] Rubí (2019: 226).

[167] Rubí (2018: 57); Egusquiza (2025: 211-212).

II. Régimen de responsabilidad civil por daños al derecho a la protección de datos personales en Chile

Tras la reforma introducida por la Ley 21.719, el párrafo quinto del título VIII de la Ley 19.628, regula el régimen de responsabilidad civil aplicable, disponiendo en su artículo 47:

> Norma 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 3°, los derechos y obligaciones establecidos en esta ley y les cause perjuicio. Lo anterior no obsta al ejercicio de los demás derechos que concede esta ley al o los titulares de datos.
>
> La acción indemnizatoria señalada en el inciso anterior podrá interponerse una vez ejecutoriada la resolución que resolvió favorablemente el reclamo interpuesto ante la Agencia o la sentencia se encuentre firme y ejecutoriada, en caso de haber presentado un reclamo de ilegalidad, y se tramitará de conformidad a las normas del procedimiento sumario establecidas en los artículos 680 y siguientes del Código de Procedimiento Civil.
>
> Las acciones civiles que deriven de una infracción a la presente ley prescribirán en el plazo de cinco años, contado desde que se encuentre ejecutoriada la resolución administrativa o la sentencia judicial, según sea el caso, que imponga la multa respectiva.

El tenor de la ley y su historia fidedigna dejan en claro que, existiendo daño, la acción indemnizatoria podrá ser deducida por la víctima una vez concluido el procedimiento administrativo, seguido ante la Agencia, cuya resolución final, conforme lo dispuesto en el artículo 43, admite reclamo judicial ante la Corte de Apelaciones correspondiente. De esta manera los hechos que originan la responsabilidad civil quedarán determinados en el procedimiento infraccional[168].

La autoridad de control en materia de protección de datos personales actúa como órgano jurisdiccional administrativo tanto en el procedimiento administrativo de tutela de derechos -artículo 41-, como en aquel sancionatorio por infracciones de ley -artículo 42- cometidos por los responsables del tratamiento de datos, para la determinación de infracciones y la imposición de sanciones, careciendo de facultades jurisdiccionales para conocer de las acciones indemnizatorias[169].

[168] Biblioteca del Congreso Nacional (2024: 365).

[169] Biblioteca del Congreso Nacional (2024: 137).

El agotamiento de la fase contencioso-administrativa previa ha sido apreciado convenientemente por la doctrina, pues permite superar los problemas de coordinación que pudieran darse en la concurrencia del derecho privado de daños con el derecho regulatorio, con la posibilidad de que un juez civil y una agencia administrativa -o en su caso el tribunal que revise su decisión- pudieran realizar apreciaciones incompatibles acerca de la comisión de una infracción de la normativa sobre protección de datos que constituye el fundamento de la obligación de indemnizar.[170]

Centrado en los principios de control de la información por parte de sus titulares y la licitud en el tratamiento de sus datos personales, ya sea en entornos físicos o digitales, las modificaciones introducidas por la Ley 21.719 adoptan el estándar europeo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales, creando una autoridad de control especializada -la Agencia- encargada de velar por la protección de los derechos y libertades de las personas titulares de datos y por el adecuado cumplimiento de las normas relativas al tratamiento de los datos; y, determinando el cumplimiento de una serie de principios, derechos y obligaciones por parte del responsable del tratamiento de datos cuya infracción, de provocar perjuicio, generará la correspondiente responsabilidad civil.

La ley adopta un modelo general de cumplimiento de la ley, responsabilidad activa o proactiva, *accountability*, sustentado en fórmulas de autorregulación tendientes a incentivar al responsable del tratamiento de datos al cumplimiento espontáneo de la legislación[171]. Es en el responsable del tratamiento en quien descansan los deberes de acreditar, en caso que sea requerido, la licitud del tratamiento; asegurar el cumplimiento del principio de finalidad; comunicar información veraz, completa y actualizada de los datos personales; de reserva y confidencialidad; de información y transparencia; de adoptar medidas de seguridad; y, de reportar las vulneraciones a las medidas de seguridad, contemplando un catálogo específico de infracciones, calificadas en leves, graves y gravísimas, estableciendo sanciones correlativas a la gravedad de la infracción[172].

Conforme el artículo 10 de la reformada Ley 19.628, los derechos reconocidos en ella se ejercen por el titular ante el responsable del tratamiento de datos, estableciendo el artículo 11 un procedimiento directo y eficaz para que cualquier titular de datos pueda recurrir directamente ante el responsable de datos, permitiéndose bloquear transitoriamente los datos en cuestión.

[170] Rubí (2019: 209).

[171] Biblioteca del Congreso Nacional (2024:120).

[172] Biblioteca del Congreso Nacional (2024: 39).

La ley, en la misma disposición, aborda diversas situaciones en que podría encontrarse el titular respecto el legitimado pasivo: pluralidad de responsables, pudiendo ejercer sus derechos ante cualquiera de ellos; responsables que sean personas jurídicas no constituidas en Chile, caso en que los responsables deberán señalar por escrito, ante la Agencia, un correo electrónico o un medio de comunicación electrónico equivalente, válido y operativo de una persona natural o jurídica capaz de actuar en su nombre, para los efectos de que el titular pueda ejercer sus derechos y comunicarse con el responsable, donde se le practiquen válidamente las comunicaciones y notificaciones administrativas que disponga la ley, debiendo los responsables mantener actualizada esta información.

El inciso tercero de la disposición que revisamos establece que los responsables de datos deberán implementar mecanismos y herramientas tecnológicas que permitan que el titular ejerza sus derechos en forma expedita, ágil y eficaz.

Si el responsable no acoge la solicitud o no responde dentro del plazo que fija la ley -conforme el artículo 11, treinta días corridos siguientes a la fecha de ingreso de la solicitud prorrogable por una vez por igual plazo-, el titular podrá presentar un reclamo ante la Agencia, conforme el procedimiento administrativo de tutela de derechos establecido en el artículo 41.

El artículo 42 establece el procedimiento para la determinación de las infracciones que cometan los responsables del tratamiento de datos por incumplimiento o vulneración de los principios, derechos y obligaciones legales y la aplicación de las sanciones correspondientes. Este procedimiento sancionatorio es instruido por la Agencia, el que podrá ser iniciado de oficio o a petición de parte, como resultado de un proceso de fiscalización o a consecuencia de una reclamación presentada por un titular de datos personales afectado. La resolución que ponga fin al procedimiento sancionatorio deberá ser fundada y contener la declaración de haberse configurado el incumplimiento o vulneración de los principios, derechos y obligaciones establecidos en la ley imponiendo la sanción correspondiente de acuerdo a la gravedad de la infracción; o, su absolución, según corresponda -artículo 42 j)-.

Conforme el artículo 43, de la resolución adoptada por la Agencia podrá deducirse reclamo de ilegalidad ante la Corte de Apelaciones de Santiago o la del domicilio del reclamante a elección de este en el plazo de quince días hábiles siguientes a la notificación de la resolución impugnada conforme las reglas que la misma disposición establece.

Si producto de la infracción de los principios, derechos y obligaciones establecidos en la ley, se causare perjuicio al titular de los datos, tiene lugar

la responsabilidad civil por el daño al derecho a la protección de datos personales o las facultades en el comprendidas, regulado en el Párrafo Quinto, artículo 47 de la Ley.

En síntesis, la Ley 21.719 ha venido a fijar un régimen de responsabilidad civil extracontractual especial, contencioso-administrativo, por daños al derecho a la protección de datos personales o derecho a la autodeterminación informativa y las prerrogativas que este comprende -derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos- derivada de un ilícito infraccional[173].

La tramitación de esta acción indemnizatoria se rige por las normas del procedimiento sumario establecidas en los artículos 680 y ss. del Código de Procedimiento Civil. A estos efectos resulta importante tener en consideración las observaciones efectuadas por la Corte Suprema dentro del proceso legislativo, oportunidad en que hizo presente la postura del Máximo Tribunal frente a los procedimientos contencioso administrativos especiales -que sería el caso de aquel seguido ante la Agencia- en torno a que la exigibilidad de la indemnización debía regirse por la regla contemplada en el literal i) del artículo 151 de la Ley de Municipalidades, el que dispone:

> Cuando se hubiere dado lugar al reclamo, el interesado podrá presentarse a los tribunales ordinarios de justicia para demandar, conforme a las reglas del juicio sumario, la indemnización de los perjuicios que procedieren y ante el Ministerio Público, la investigación criminal que correspondiere. En ambos casos, no podrá discutirse la ilegalidad ya declarada.

La Corte Suprema en su oficio de 3 de mayo de 2017, numeral decimotercero, hace presente que "[D]e este modo se incentivaría el uso de esta acción, ahorrando los costos que implica un juicio ordinario, y evitando posibles dilaciones injustas para el titular"[174], procedimiento aplicable que, en definitiva, recoge la Ley.

[173] Corral (2004: 271 - 272).

[174] Biblioteca del Congreso Nacional (2024: 79).

III. Acción indemnizatoria en la Ley 21.719

1. Legitimación activa

Conforme las reglas introducidas por la Ley 21.719 la legitimación activa corresponde al o los titulares de los datos, esto es la persona natural, identificada o identificable, a quien conciernen o se refieren los datos personales -artículo 2 ñ-. Las víctimas legitimadas para el ejercicio de la acción lo son por la afectación directa de sus datos personales.

2. Legitimación pasiva

El responsable del tratamiento de datos es el legitimado pasivo de la acción, conforme el literal n) del artículo 2 corresponde a "toda persona natural o jurídica, pública o privada, que decide acerca de los fines y 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".

El tercero mandatario o encargado es la persona natural o jurídica que trata datos personales, por cuenta del responsable de datos -artículo 2 x)-.

El artículo 15 bis de la Ley se dedica al tratamiento de datos a través de un tercero mandatario o encargado, estableciendo en su inciso tercero que, si este trata los datos con un objeto distinto del encargo convenido o los cede o entrega sin haber sido autorizado, se le considerará como responsable para todos los efectos legales. La norma lo hace responsable en forma personal respecto las infracciones que cometa y, solidariamente con el responsable por los daños derivados de la infracción, sin perjuicio de las responsabilidades contractuales para con su mandante.

En lo tocante a la cesión de datos personales, el artículo 15 de la modificada Ley 19.628, dispone que una vez esta perfeccionada,

> [E]l cesionario adquiere la condición de responsable de datos para todos los efectos legales. El cedente, por su parte, también mantiene la calidad de responsable de datos, respecto de las operaciones de tratamiento que continúe realizando. Si se verifica una cesión de datos sin contar con el consentimiento del titular, siendo éste necesario, la cesión será nula, debiendo el cesionario suprimir todos los datos recibidos, sin perjuicio de las responsabilidades legales que correspondan.

Consecuentemente, por la cesión válidamente efectuada, el cesionario será el responsable del tratamiento de datos. Si la cesión no cuenta con la debida autorización del titular de los datos, podrá también el cesionario ser sujeto pasivo de la acción indemnizatoria por los daños provocados con la infracción.

3. Factor de imputación: la culpa infraccional o culpa contra la legalidad

El factor de imputación de la responsabilidad civil en la materia fue abordado por la doctrina nacional con ocasión de la disposición contenida en el texto original de la Ley 19.628 que dedicaba su Título V a la responsabilidad por las infracciones a la misma ley, prescribiendo en el artículo 23 que "La persona natural o jurídica privada o el organismo público responsable del banco de datos personales deberá indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de los datos […]". Las observaciones respecto a la utilización por el legislador del tono imperativo -que reitera en el actual artículo 47- se planteaban en torno a que este podría inducir a pensar que se trataría de un caso de responsabilidad objetiva, interpretación que se descarta en atención a que la responsabilidad que establece deriva de un ilícito infraccional, el que sólo procede cuando se acredita el elemento subjetivo[175].

La culpa infraccional o culpa contra la legalidad es un criterio de atribución de responsabilidad civil extracontractual o categoría especial de culpabilidad que consiste en imputar la contravención de una norma jurídica específica del ordenamiento que establece un deber de cuidado, de cuya verificación positiva se derivaría como consecuencia o efecto jurídico paradigmático una presunción general de culpabilidad en favor de la víctima del daño, la que impondría, al agente infractor, la carga procesal de desvirtuarla mediante la acreditación del cumplimiento de la diligencia debida.[176]

Barros indica como una práctica común el que por vía legislativa sean reguladas actividades que presentan riesgos, siendo las consideraciones del legislador esencialmente preventivas[177]. En este sentido, las modificaciones introducidas a la Ley de Protección de Datos instauran un régimen de responsabilidad activa de los responsables del tratamiento de datos, dado que el tratamiento de datos se concibe como una actividad generadora de

[175] Corral (2004: 272).
[176] Bassi (2017: 37 – 38).
[177] Barros (2010: 98).

riesgos, se considera a quien adopta las decisiones básicas al respecto como responsable último de todos los daños que supongan una materialización de los riesgos inherentes a las operaciones sobre datos personales.[178]

La infracción a las disposiciones legales, en el caso que revisamos, los principios, derechos y obligaciones establecidos por la Ley 21.719 genera una presunción de culpa que, conforme la doctrina mayoritaria, sitúa al transgresor de la norma -el responsable del tratamiento de datos personales- en la necesidad de acreditar la debida diligencia[179].

La culpa infraccional es una presunción de culpabilidad que puede ser desvanecida por hechos justificatorios. Conforme los principios generales del derecho privado la infracción a un deber legal puede ser excusada recurriendo a causales de justificación[180], que operarán como excepciones justificatorias de la conducta que *per se* se tiene por ilícita, las que deberá probar quien las alega, siendo de común aceptación en doctrina la ejecución de actos autorizados por el derecho; el consentimiento de la víctima; el estado de necesidad, y la legítima defensa.[181]

4. Carga de la prueba

Como hemos señalado, con el objeto de reforzar la legitimidad del tratamiento de datos, la Ley establece una serie de obligaciones y deberes para los responsables de datos, tales como acreditar la licitud del tratamiento que realizan; deberes de información; deberes de reserva y confidencialidad, de información y transparencia, y el deber de adoptar medidas de seguridad y reportar las vulneraciones dichas medidas.[182] Resulta de interés hacer notar que la Ley, en el artículo 48 establece, además, un régimen de prevención de infracciones de cargo de los responsables del tratamiento de datos quienes deberán adoptar acciones destinadas a prevenir la comisión de infracciones calificadas como leves, graves y gravísimas que se detallan en los artículos 34 bis, 34 ter y 34 quáter, respectivamente.

En este sentido, concordante con la premisa estructurante de que los datos personales deben estar bajo la esfera de control de su titular, la normativa establece el consentimiento como la fuente principal de legitimidad del tratamiento de los datos personales. En este sentido, el principio de licitud y lealtad contenido en la letra a) del artículo 3, prescribe que el responsable del

[178] Rubí (2018: 62).
[179] Bassi (2017: 44).
[180] Barros (2010: 99).
[181] Barros (2010: 133).
[182] Biblioteca del Congreso Nacional (2024: 37).

tratamiento de datos deberá ser capaz de acreditar la licitud del tratamiento de datos personales que realiza, radicando en este la carga de "probar que contó con el consentimiento del titular y que el tratamiento de datos fue realizado en forma lícita, leal y transparente" -artículo 12 inciso final-. Así, habiendo adoptado la ley un modelo general de cumplimiento, dentro del procedimiento administrativo por infracción de ley seguido ante la Agencia, será al responsable del tratamiento de datos a quien corresponderá la prueba.

Determinada la infracción en la resolución de término en el procedimiento administrativo o en la sentencia pronunciada en el procedimiento de reclamación judicial, si es que con ella se causó un daño al titular en su derecho a la protección de datos personales, procede el ejercicio de la acción indemnizatoria ante el tribunal civil competente. Desde este punto de vista el titular contará, desde ya, con uno de los elementos para configurar la responsabilidad civil: la infracción a los principios, derechos u obligaciones establecidas por la ley de protección de datos personales. Luego, para hacer nacer la responsabilidad civil establecida en el artículo 47, la víctima, titular del derecho a la protección de datos personales dañado, deberá probar el perjuicio provocado y la relación de causalidad entre la infracción cometida por el responsable y el daño sufrido.

En el juicio de indemnización de perjuicios por el daño al derecho a la protección de datos personales, la víctima deberá probar: la infracción legal -hecho ilícito- lo que acreditará con la infracción determinada y la sanción impuesta por resolución final de la Agencia o la sentencia firme y ejecutoriada del reclamo de ilegalidad; el daño cierto sufrido; el nexo de causalidad entre la infracción -el hecho ilícito- y el daño. Tratándose de un supuesto de culpa infraccional, la culpa del infractor se presume invirtiendo la carga de la prueba, debiendo el demandado acreditar la diligencia -cuestión en que tendrá importancia el cumplimiento del principio de responsabilidad proactiva- o, los hechos en que funde alguna causal de exoneración.

El responsable del tratamiento de datos personales también podrá probar los hechos en que funde la falta de nexo causal -caso fortuito o fuerza mayor, hecho exclusivo de la víctima, hecho de un tercero- o la inexistencia del daño alegado.

5. Daño indemnizable y modalidad de reparación

El artículo 47 de la Ley dispone la indemnización de los daños tanto patrimoniales como extrapatrimoniales derivados de la infracción cometida por el responsable, los que deberán ser probados en juicio, correspondiendo al órgano jurisdiccional su determinación y avaluación.

En efecto, como hemos podido revisar del antecedente legislativo constituido por el RGPD, la sola infracción de principios y derechos no constituye

por sí misma elemento suficiente para reclamar una indemnización de perjuicios, sino se requiere la existencia real y efectiva del daño.

El legislador nacional, entre las modificaciones introducidas por la Ley 21.719, avanza en considerar los daños extrapatrimoniales, abriendo la taxonomía de daños que pudieren comprenderse en la categoría, superando la restringida noción de daño moral, particularmente relevante en materia de daños a derechos de la personalidad[183].

Probado el daño producido, reunidos los requisitos para la aplicación del régimen de responsabilidad civil extracontractual especial que analizamos, debe atenderse a su reparación guiada por el principio de reparación integral del daño, ámbito de justicia correctiva "que pretende restablecer, en la relación entre el demandado y la víctima, el orden que ha sido alterado por el daño"[184].

En cuanto a las modalidades de la reparación del daño producido, teniendo en consideración la especial naturaleza del derecho vulnerado, más allá de la indemnización en metálico o monetaria, se advierte -a efectos de la efectiva vigencia de la máxima de reparación integral- la procedencia y complementariedad de la reparación en naturaleza, *in natura* o específica, la que apunta a restablecer la situación que existía con anterioridad a la producción del daño, adoptando medidas ya sea, de restitución, de satisfacción o de rehabilitación[185], consistentes "en la obligación del responsable de ejecutar una o varias prestaciones no pecuniarias dirigidas a reconstruir o restaurar física o económicamente la situación jurídica que el perjudicado tendría de no haber ocurrido el hecho dañoso"[186], las que resultan admisible en el sistema interno de la mano de los artículos 2314 y 2329 inciso primero del código civil[187].

Respecto la reparación del daño al derecho a la protección de datos personales, se han identificado como formas de reparación *in natura*, a modo ejemplar, la publicación de la sentencia condenatoria del infractor o las disculpas públicas.[188]

[183] Álvarez y Prado (2023: 118-119).
[184] Barros (2010: 215).
[185] Álvarez y Prado (2023: 143-145).
[186] Tapia (2013:31).
[187] Álvarez y Prado (2023:145).
[188] Riveros y López (2025: 275).

6. Prescripción

El inciso final del artículo 47 dispone, "Las acciones civiles que deriven de una infracción a la presente ley prescribirán en el plazo de cinco años, contado desde que se encuentre ejecutoriada la resolución administrativa o la sentencia judicial, según sea el caso, que imponga la multa respectiva".

IV. Jurisprudencia nacional: Breve revisión de aspectos relevantes en torno a la responsabilidad civil extracontractual por daños al derecho a la protección de datos personales en vigencia de la Ley 19.628.

Hasta la fecha, las sentencias de los altos tribunales nacionales han aplicado en materia de responsabilidad civil por daños al derecho a la protección de datos personales las disposiciones vigentes, contenidas en la Ley 19.628. No obstante, es posible reconocer en ellas aspectos relevantes en torno a la concurrencia de los requisitos de la responsabilidad civil, la prueba del daño y los deberes de los responsables del tratamiento de datos, los que pasamos a revisar:

En sentencia de la CS, de 3 de julio de 2020 dictada en causa rol N°17.667-2019, particularmente, respecto el recurso de casación en el fondo deducido por Sistema Nacional de Comunicaciones Financieras S.A (SINACOFI S.A.) en contra de la sentencia de 26 de abril de 2019 de la Corte de Apelaciones de Temuco, causa rol N°698-2018, establece que la demandada, en atención a lo dispuesto por la Ley 19.228, realizó un indebido tratamiento de datos personales del demandante al publicar dos facturas sin su consentimiento, las que además fueron impugnadas por falsedad, lo que le ocasionó perjuicios susceptibles de ser indemnizados -considerando noveno-, constituyendo una infracción al artículo 23 de la Ley 19.628, por lo que en el considerando duodécimo concluye que, "la obligación de reparar los perjuicios causados impuesta al responsable del cuidado de los datos, no exime al afectado de la carga de acreditar su existencia y monto, lo que en el caso, de acuerdo a los hechos establecidos en la sentencia, ocurrió".

La sentencia dictada por la I. Corte de Apelaciones de Temuco revoca la sentencia de primera instancia y en su lugar resuelve la indemnización de perjuicios en favor del demandante fijando prudencialmente su monto en $500.000 (el monto de los perjuicios por daño moral esgrimido por el demandante ascendía a $20.000.000). El fallo de segunda instancia de 26 de abril de 2019 en su considerando tercero señala:

> Que conforme lo dispone la Ley 19.628 en su Artículo 23 para que proceda la indemnización de perjuicios por daño, es supuesto necesario que ocurra un tratamiento indebido de datos comerciales como hecho ilícito que lo origina, debiendo también y en todo caso estar presentes los otros elementos necesarios para que se genere responsabilidad civil, en este caso extracontractual, a saber, perjuicios o daño, nexo causal, capacidad civil de tipo delictual de los Artículos 2314 y siguientes del Código Civil.

Para continuar en su considerando séptimo indicando,

> Que, el Artículo 2° letra o) de la Ley 19.628 define lo que debe entenderse por tratamiento de datos personales como: "cualquier manejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma". De este modo, la demandada SINACOFI S.A., ha expuesto que se dedicaría a la transmisión de mensajes electrónicos y otros para la industria bancaria, dicha transmisión, no es más que la comunicación de información que le permite a las instituciones financieras tomar decisiones de tipo crediticio, de manera que SINACOFI S.A. efectúa tratamiento de datos personales de carácter económico al dedicarse a transmitir información de tipo financiero a instituciones bancarias, por lo cual debe observar estrictamente lo dispuesto en la Ley 19.268 pudiendo publicar única y exclusivamente aquellos documentos enumerados en forma taxativa por la ley en su Artículo 17, dentro de los cuáles no se encuentran las facturas, que en este caso fueron tratadas por la demandada conjuntamente con Fidelidad SpA, estimando este tribunal que el actuar ilícito se encuentra acreditado en conformidad a la norma enunciada.

La sentencia en comento identifica correctamente los elementos para que la responsabilidad civil extracontractual sea procedente en el caso, teniendo como presupuesto la infracción, hecho ilícito, cometido por el responsable del tratamiento de datos, considerando la presunción de culpabilidad derivada del supuesto de culpa infraccional que entraña, como se desprende del considerando octavo el que indica:

> Que, la ley 19.628 Sobre Protección de Vida Privada, precisamente lo que pretende es hacer patente el derecho constitucional que tienen todas las personas de que se resguarde su vida privada y su honra, siendo el tratamiento de datos personales una excepción permitida única y exclusivamente para fines estadísticos, legales, bajo el consentimiento

> de su titular en el caso de datos sensibles o para resguardar el buen funcionamiento del mercado del dinero respecto del tratamiento de datos financieros como es el caso, debiendo por ende ser la publicación de dichos datos en extremo restrictiva para no afectar la garantía fundamental del n° 4 del Artículo 19 de la Constitución Política de la República enunciada al inicio de este considerando, de ahí que esta ley especial permite incluso apreciar la prueba en conciencia por el sentenciador, *rebajando considerablemente la carga de la prueba para quien se vea afectado en este derecho* (énfasis añadido).

La sentencia, sin embargo, no distingue el derecho a la protección de datos personales lesionado del derecho a la intimidad, los que aborda conjuntamente como se desprende del considerando anterior transcrito, confusión que se observa también en el considerando siguiente al señalar,

> NOVENO: Que, corresponde verificar si concurren en la especie los otros elementos que permiten acceder a una indemnización de perjuicios, dando por sentada la capacidad para ser responsables civilmente de los demandados, correspondiendo pronunciarse sobre la existencia o no de una relación de causalidad entre el hecho ilegal de haber publicado documentos no permitidos *y el daño, que en este tipo de casos es el daño a la honra como base*, lo que puede tener repercusiones materiales como es lo alegado aquí en que la honra comercial del actor se vio afectada y tuvo repercusiones económicas al privarlo de acceder a créditos y seguros, pero no es el valor de esos productos bancarios lo que reclama, lo reclamado es la afectación de su honra como comerciante que cumple con sus obligaciones (énfasis añadido).

El 09 de septiembre de 2025, la CS se pronuncia en causa rol N°30.842-2025, caratulada "Medina con Entel PCS Comunicaciones S.A.", rechazando el recurso de casación deducido por la demandada en contra de la sentencia de la Corte de Apelaciones de Santiago que confirmó la sentencia de primera instancia acogiendo la indemnización de perjuicios con declaración de aumentar su monto a $7.000.000. El 5° Juzgado civil de Santiago en su sentencia había determinado prudencialmente el monto del daño moral en la suma de $600.000.

Los hechos asentados por la judicatura de fondo dan cuenta que, en abril de 2019, el demandante dejó de ser cliente de Entel PCS Telecomunicaciones S.A., tras lo cual terceras personas se valieron de sus datos personales para contratar líneas telefónicas a su nombre, sin su consentimiento. Acogiéndose la demanda se tuvo por acreditado que "la parte demandada *no otorgó el debido cuidado a los datos personales del demandante*, [por lo que] le resulta

aplicable lo dispuesto en artículo 23 de la Ley 19628, esto es, el deber de indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de los datos" (énfasis añadido), lo que el Máximo Tribunal destaca en el considerando tercero de su sentencia, determinando, en definitiva, que los tribunales del fondo efectuaron una correcta aplicación de las normas jurídicas pertinentes al caso, por lo que no cabe sino concluir la desestimación del recurso de casación interpuesto por la demandada por adolecer de manifiesta falta de fundamento (considerando quinto).

GLOSARIO

Agencia de Protección de Datos Personales: Corporación autónoma de derecho público, de carácter técnico, 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, teniendo por objeto velar por la efectiva protección de los derechos que garantizan la vida privada de las personas y sus datos personales, de conformidad a lo establecido en la Ley 19.628 sobre protección de datos personales, y fiscalizar el cumplimiento de sus disposiciones (artículo 30 Ley 19.628 sobre protección de datos personales).

Almacenamiento de datos: La conservación o custodia de datos en un registro o base de datos (artículo 2 letra a) Ley 19.628 sobre protección de los datos personales).

Anonimización: 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 (artículo 2 letra k) Ley 19.628 sobre protección de los datos personales).

Base de datos personales: Conjunto organizado de datos personales, cualquiera sea la finalidad, forma o modalidad de su creación, almacenamiento, organización y acceso, que permita relacionar los datos entre sí, así como realizar su tratamiento (artículo 2 letra m) Ley 19.628 sobre protección de los datos personales).

Bloqueo de datos: La suspensión temporal de cualquier operación de tratamiento de los datos almacenados (artículo 2 letra b) Ley 19.628 sobre protección de los datos personales).

Cesión de datos personales: Transferencia de datos personales por parte del responsable de datos a otro responsable de datos (artículo 2 letra v) Ley 19.628 sobre protección de los datos personales).

Cesión de datos personales por un órgano público: La facultad de los organismos públicos para ceder datos personales específicos, o todo o parte

de sus bases de datos o conjuntos de datos, a otros órganos públicos, para un tratamiento específico, de forma que el órgano receptor no los podrá utilizar para otros fines, y siempre que la cesión de los datos resulte necesaria para el cumplimiento de sus funciones legales y ambos órganos actúen dentro del ámbito de sus competencias (artículo 22 Ley 19.628 sobre protección de los datos personales).

Comunicación de datos personales: Dar a conocer por el responsable de datos, de cualquier forma, datos personales a personas distintas del titular a quien conciernen los datos, sin llegar a cederlos o transferirlos (artículo 2 letra c) Ley 19.628 sobre protección de los datos personales).

Comunicación de datos personales por un órgano público: Facultad de los organismos públicos para comunicar datos personales específicos, o todo o parte de sus bases de datos o conjuntos de datos, a otros órganos públicos, para un tratamiento específico, de forma que el órgano receptor no los podrá utilizar para otros fines, y siempre que la comunicación de los datos resulte necesaria para el cumplimiento de sus funciones legales y ambos órganos actúen dentro del ámbito de sus competencias (artículo 22 Ley 19.628 sobre protección de los datos personales).

Consentimiento: Toda manifestación de voluntad libre, específica, inequívoca e informada, otorgada a través de una declaración o una clara acción afirmativa, mediante la cual el titular de datos, su representante legal o mandatario, según corresponda, autoriza el tratamiento de los datos personales que le conciernen (artículo 2 letra p) Ley 19.628 sobre protección de los datos personales).

Dato caduco: El que ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia o, si no hubiese norma expresa, por el cambio de los hechos o circunstancias que consigna (artículo 2 letra d) Ley 19.628 sobre protección de los datos personales).

Dato estadístico: El dato que, en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable (artículo 2 letra e) Ley 19.628 sobre protección de los datos personales).

Dato personal: 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. Para determinar si una persona es identificable deberán considerarse todos

los medios y factores objetivos que razonablemente se podrían usar para dicha identificación en el momento del tratamiento (artículo 2 letra f) Ley 19.628 sobre protección de los datos personales).

Datos personales biométricos: Aquellos datos personales sensibles obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona que permitan o confirmen la identificación única de ella, tales como la huella digital, el iris, los rasgos de la mano o faciales y la voz (artículo 16 ter Ley 19.628 sobre protección de los datos personales).

Datos personales con fines históricos, estadísticos, científicos y de estudios o investigaciones: Aquellos datos personales cuyo tratamiento sea realizado por personas naturales o jurídicas, públicas o privadas, incluidos los organismos públicos, cuando el tratamiento tenga un interés legítimo, es decir, cuando se realiza exclusivamente con fines históricos, estadísticos, científicos y para estudios o investigaciones, todos los cuales deben atender fines de interés público (artículo 16 quinquies Ley 19.628 sobre protección de los datos personales).

Datos relativos a infracciones penales, civiles, administrativas y disciplinarias: Aquellos datos personales relativos a la comisión y sanción de infracciones penales, civiles, administrativas y disciplinarias (artículo 25 Ley 19.628 sobre protección de los datos personales).

Datos personales relativos a los niños, niñas y adolescentes: Cualquier dato personal que concierna a los niños, niñas y adolescentes (artículo 16 quáter Ley 19.628 sobre protección de datos personales).

Datos personales sensibles: Tendrán esta condición aquellos datos personales que refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, que revelen el origen étnico o racial, la afiliación política, sindical o gremial, la situación socioeconómica, las convicciones ideológicas o filosóficas, las creencias religiosas, los datos relativos a la salud, al perfil biológico humano, los datos biométricos, y la información relativa a la vida sexual, a la orientación sexual y a la identidad de género de una persona natural (artículo 2 letra g) Ley 19.628 sobre protección de los datos personales).

Datos personales sensibles relativos a la salud y al perfil biológico humano: Cualquier información vinculada o referida a la salud y perfil biológico del titular, como los datos genéticos, proteómicos o metabólicos (artículo 16 bis Ley 19.628 sobre protección de datos personales).

Deber de adoptar medidas de seguridad: Deber del responsable de datos conforme al cual debe adoptar las medidas necesarias para resguardar el cumplimiento del principio de seguridad establecido en la Ley 19.628 sobre protección de los datos personales, considerando el estado actual de la técnica y los costos de aplicación, junto con la naturaleza, alcance, contexto y fines del tratamiento, así como la probabilidad de los riesgos y la gravedad de sus efectos en relación con el tipo de datos tratados (artículo 14 quinquies Ley 19.628 sobre protección de los datos personales).

Deber de información y transparencia: Deber del responsable de datos conforme al cual está obligado a facilitar y mantener permanentemente a disposición del público, en su sitio web o en cualquier otro medio de información equivalente, al menos la información señalada en el artículo 14 ter de la Ley 19.628 sobre protección de los datos personales (artículo 14 ter Ley 19.628 sobre protección de los datos personales).

Deber de protección desde el diseño y por defecto: Deber del responsable de datos conforme al cual está obligado a aplicar medidas técnicas y organizativas adecuadas desde el diseño con anterioridad y durante el tratamiento de los datos personales (artículo 14 quáter Ley 19.628 sobre protección de los datos personales).

Deber de reportar las vulneraciones a las medidas de seguridad: Deber del responsable de datos conforme al cual deberá reportar a la Agencia de Protección de Datos, por los medios más expeditos posibles y sin dilaciones indebidas, las vulneraciones a las medidas de seguridad que ocasionen la destrucción, filtración, pérdida o alteración accidental o ilícita de los datos personales que trate o la comunicación o acceso no autorizados a dichos datos, cuando exista un riesgo razonable para los derechos y libertades de los titulares (artículo 14 sexies Ley 19.628 sobre protección de los datos personales).

Deber de secreto o confidencialidad: Deber del responsable de datos conforme al cual está obligado a mantener secreto o confidencialidad acerca de los datos personales que conciernan a un titular, salvo cuando el titular los hubiere hecho manifiestamente públicos (artículo 14 bis Ley 19.628 sobre protección de los datos personales).

Delegado de protección de datos personales: Persona designada por el responsable de datos en el modelo de prevención de infracciones para que cumpla con las funciones y atribuciones que la Ley 19.628 sobre protección de los datos personales le otorga en su artículo 50 (artículos 49 letra a) y 50 Ley 19.628 sobre protección de los datos personales).

Derecho a la portabilidad de los datos personales: 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. El titular tendrá derecho a que sus datos personales se transmitan directamente de responsable a responsables cuando sea técnicamente posible (artículo 2 letra u) Ley 19.628 sobre protección de los datos personales).

Derecho de acceso: 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 (artículo 2 letra q) Ley 19.628 sobre protección de los datos personales).

Derecho de bloqueo: Derecho del titular de datos 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 (artículo 8° ter Ley 19.628 sobre protección de los datos personales).

Derecho de oposición: Derecho del titular de datos 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 (artículo 2 letra t) Ley 19.628 sobre protección de los datos personales).

Derecho de rectificación: 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 (artículo 2 letra r) Ley 19.628 sobre protección de los datos personales).

Derecho de supresión: Derecho del titular de datos a solicitar y obtener del responsable, que suprima o elimine sus datos personales, de acuerdo a las causales previstas en la ley (artículo 2 letra s) Ley 19.628 sobre protección de los datos personales).

Elaboración de perfiles: Toda forma de tratamiento automatizado de datos personales que consista en utilizar esos datos para evaluar, analizar o predecir aspectos relativos al rendimiento profesional, situación económica, de salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de una persona natural (artículo 2 letra v) Ley 19.628 sobre protección de los datos personales).

Eliminación o cancelación de datos: La destrucción de datos almacenados en registros o bancos de datos, cualquiera fuere el procedimiento

empleado para ello (artículo 2 letra h) Ley 19.628 sobre protección de los datos personales).

Evaluación de impacto en protección de datos personales: Proceso que debe ser realizado por el responsable del tratamiento de datos personales, previo al inicio de las operaciones del tratamiento, en los casos expresamente señalados en el artículo 15 ter de la Ley 19.628 sobre protección de los datos personales o cuando sea probable que un tipo de tratamiento, por su naturaleza, alcance, contexto, tecnología utilizada o fines, pueda producir un alto riesgo para los derechos de las personas titulares de los datos personales (artículo 15 ter Ley 19.628 sobre protección de los datos personales).

Fuentes de acceso público: Todas aquellas bases de datos o conjuntos de datos personales, cuyo acceso o consulta puede ser efectuada en forma lícita por cualquier persona, tales como el Diario Oficial, medios de comunicación o los registros públicos que disponga la ley. El tratamiento de datos personales provenientes de fuentes de acceso público se someterá a las disposiciones de esta ley ((artículo 2 letra i) Ley 19.628 sobre protección de los datos personales).

Infracciones graves: Aquellas infracciones a la Ley 19.628 sobre protección de los datos personales descritas en su artículo 34 ter y que serán sancionadas con amonestación escrita o multa de hasta 5.000 unidades tributarias mensuales (artículos 34 ter y 35 Ley 19.628 sobre protección de los datos personales).

Infracciones gravísimas: Aquellas infracciones a la Ley 19.628 sobre protección de los datos personales descritas en su artículo 34 quáter y que serán sancionadas con amonestación escrita o multa de hasta 5.000 unidades tributarias mensuales (artículos 34 quáter y 35 Ley 19.628 sobre protección de los datos personales).

Infracciones leves: Aquellas infracciones a la Ley 19.628 sobre protección de los datos personales descritas en su artículo 34 bis y que serán sancionadas con amonestación escrita o multa de hasta 5.000 unidades tributarias mensuales (artículos 34 bis y 35 Ley 19.628 sobre protección de los datos personales).

Modelo de prevención de infracciones: Programa de cumplimiento que los responsables de datos podrán voluntariamente adoptar para prevenir infracciones (artículo 49 Ley 19.628 sobre protección de datos personales).

Organismos públicos: Las autoridades, órganos del Estado y organismos, descritos y regulados por la Constitución Política de la República, y los comprendidos en el inciso segundo del artículo 1° de la Ley 18.575, Orgánica

Constitucional de Bases Generales de la Administración del Estado (artículo 2 letra j) Ley 19.628 sobre protección de los datos personales).

Principio de calidad: Principio jurídico conforme al cual los datos personales deben ser exactos, completos, actuales y pertinentes en relación con su proveniencia y los fines del tratamiento (artículo 3 letra d) Ley 19.628 sobre protección de los datos personales).

Principio de confidencialidad: Principio jurídico conforme al cual el responsable de datos personales y quienes tengan acceso a ellos deberán guardar secreto o confidencialidad acerca de los mismos (artículo 3 letra h) Ley 19.628 sobre protección de los datos personales).

Principio de coordinación: Principio jurídico conforme al cual los organismos públicos deben alcanzar un alto grado de interoperabilidad y coherencia, de modo de evitar contradicciones en la información almacenada y reiteración de requerimientos de información o documentos a los titulares de datos (artículo 21 inciso segundo Ley 19.628 sobre protección de los datos personales).

Principio de eficiencia: Principio jurídico conforme al cual los organismos públicos deben evitar la duplicación de procedimientos y trámites entre los organismos públicos y entre éstos y los titulares de la información (artículo 21 inciso segundo Ley 19.628 sobre protección de los datos personales).

Principio de finalidad: Principio jurídico conforme al cual los datos personales deben ser recolectados con fines específicos, explícitos y lícitos (artículo 3 letra b) Ley 19.628 sobre protección de los datos personales).

Principio de proporcionalidad: Principio jurídico conforme al cual los datos personales que se traten deben limitarse estrictamente a aquellos que resulten necesarios, adecuados y pertinentes en relación con los fines del tratamiento (artículo 3 letra c) Ley 19.628 sobre protección de los datos personales).

Principio de responsabilidad: Principio jurídico conforme al cual quienes realicen tratamiento de los datos personales serán legalmente responsables del cumplimiento de los principios contenidos en la ley 19.928 sobre protección de los datos personales (artículo 3 letra e) Ley 19.628 sobre protección de los datos personales).

Principio de seguridad: Principio jurídico conforme al cual, en el tratamiento de los datos personales, el responsable debe garantizar estándares adecuados de seguridad, protegiéndolos contra el tratamiento no autorizado o ilícito, y contra su pérdida, filtración, daño accidental o destrucción. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento

que se vaya a efectuar y con la naturaleza de los datos (artículo 3 letra f) Ley 19.628 sobre protección de los datos personales).

Principio de transparencia e información: Principio jurídico conforme al cual el responsable debe entregar al titular toda la información que sea necesaria para el ejercicio de los derechos que establece la Ley 19.628 sobre protección de los datos personales, incluyendo las políticas y las prácticas sobre el tratamiento de los datos personales, las que además deberán encontrarse permanentemente accesibles y a disposición de cualquier interesado de manera precisa, clara, inequívoca y gratuita (artículo 3 letra g) Ley 19.628 sobre protección de los datos personales).

Principios de licitud y lealtad: Principio jurídico conforme al cual los datos personales solo pueden tratarse de manera lícita y leal. Es lícito el tratamiento de datos personales, sin el consentimiento del titular, en los casos enumerados en el artículo 13 de la Ley 19.628 sobre protección de los datos personales (artículo 3 letra a) Ley 19.628 sobre protección de los datos personales).

Registro Nacional de Sanciones y Cumplimiento: Es un registro nacional de carácter público administrado por la Agencia, que consigna los modelos certificados de prevención, los responsables de datos que los hayan adoptado y las sanciones que se hayan impuesto a los responsables de datos que hayan infringido la ley (artículo 2 letra z) Ley 19.628 sobre protección de los datos personales).

Representante legal o mandatario: Persona natural o jurídica designada por el titular de datos personales para obrar a su nombre o representación en el ejercicio de los derechos conferidos por la Ley 19.628 sobre protección de los datos personales.

Responsable de datos o responsable: 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 (artículo 2 letra n) Ley 19.628 sobre protección de los datos personales).

Sanciones accesorias: Aquellas sanciones que la Ley 19.628 dispone que podrán ser aplicadas por la Agencia en los casos en que se impongan multas por infracciones gravísimas reiteradas, en un período de veinticuatro meses, y que consisten en la suspensión de las operaciones y actividades de tratamiento de datos que realiza el responsable de datos, hasta por un término de treinta días, sin afectar al almacenamiento de datos (artículo 38 Ley 19.628 sobre protección de los datos personales).

Seudonimización: 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 organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona natural identificada o identificable (artículo 2 letra l) Ley 19.628 sobre protección de los datos personales).

Tercero mandatario o encargado: La persona natural o jurídica que trate datos personales, por cuenta del responsable de datos (artículo 2 letra x) Ley 19.628 sobre protección de los datos personales).

Titular de datos o titular: Persona natural, identificada o identificable, a quien conciernen o se refieren los datos personales (artículo 2 letra ñ) Ley 19.628 sobre protección de los datos personales).

Tratamiento de datos: Cualquier operación o conjunto de operaciones o procedimientos o técnicos, de carácter automatizado o no, que permitan de cualquier forma recolectar, procesar, almacenar, comunicar, transmitir o utilizar datos personales o conjuntos de datos personales (artículo 2 letra o) Ley 19.628 sobre protección de los datos personales).

EJERCICIOS DE APLICACIÓN PRÁCTICA: PREGUNTAS Y RESPUESTAS

1. **María Morales es una mujer de 37 años que, hace unos 5 años, cuando vivía en La Serena, se suscribió al boletín electrónica de una tienda online llamada "Electrónica La Serena", proporcionando su nombre completo, dirección, teléfono, correo electrónico y algunos datos sobre sus preferencias de productos, específicamente, marcas, tipos de productos, rangos de precios. Recientemente, descubrió que sus datos fueron cedidos a una empresa de envíos, sin que ella hubiera autorizado expresamente esa cesión, para efectos de marketing, por lo cual empezó a recibir publicidad de esta nueva empresa. ¿Qué puede hacer considerando la nueva ley de protección de datos?**

En este caso, se encuentra involucrado el *derecho de oposición* regulado en el artículo 8 de la Ley 19.628 sobre protección de datos personales.

María puede ejercer este derecho contra la empresa de envíos para oponerse a que sus datos sean tratados para ciertos fines específicos, como el de marketing, causal que está expresamente considerada en la letra b) del citado artículo 8.

También puede solicitarle a esta empresa el ejercicio de su *derecho de supresión*, establecido en el artículo 7°, para que se eliminen sus datos personales, invocando la causal establecida en la letra f), esto es, cuando el titular haya ejercido su derecho de oposición de conformidad al artículo 8° y no exista otro fundamento legal para su tratamiento. Si la empresa no responde o niega la solicitud, María puede recurrir a la Agencia de Protección de Datos, a través del procedimiento del artículo 41 de la nueva ley, para el ejercicio de sus derechos.

Además, como la cesión fue sin su consentimiento, se ha infringido lo dispuesto en el Artículo 12 respecto del consentimiento del titular establecido en los artículos 12 y 15 de la ley. Por lo tanto, puede denunciar la infracción de la empresa Electrónica La Serena a la Agencia de Protección de Datos, aplicando el procedimiento establecido en el artículo 42 de la mencionada ley. La cesión de datos personales sin el consentimiento del titular en los casos que sea necesario o para un fin distinto al autorizado constituye una infracción grave consagrada en la letra b) del artículo 34 ter de la ley, cuya

sanción corresponde a una multa superior a 5.000 UTM hasta 10.000 UTM, sin perjuicio de las medidas que la Agencia disponga tendientes a subsanar las causales que dieron motivos a la sanción o de la imposición de sanciones accesorias.

Con todo, mientras se tramitan todos estos procedimientos, María puede solicitar la suspensión temporal de cualquier operación de tratamiento de sus datos personales, a través del *derecho de bloqueo del tratamiento*, establecido en el artículo 8° ter de la ley.

2. Raúl Fuentes, de 64 años, asiste regularmente a la "Clínica Sentirse Bien" para sus chequeos médicos. La Clínica tiene un portal de internet en donde los pacientes pueden ingresar con su cédula de identidad y una contraseña creada por ellos, y está toda su ficha online, incluyendo horas médicas, resultados de exámenes, diagnósticos, medicamentos recetados, fechas para agendar próximos controles, recomendaciones e indicaciones y en general toda información médica que resulte de las visitas a la Clínica. El señor Fuentes tiene una enfermedad crónica que requiere controles frecuentes y medicamentos de uso permanente. En el último tiempo, el señor Fuentes empieza a recibir publicidad de medicamentos específicos para su enfermedad a través de redes sociales y correos electrónicos. Por ello, sospecha que la clínica compartió su información médica, especialmente en lo referido a su diagnóstico y tratamientos.

Además, al revisar su ficha clínica en línea, luego de su último control, se dio cuenta de que aparecen resultados de exámenes anteriores, por sobre los últimos que se realizó, lo que generó confusión en su último control, ya que los primeros se presentan como los más recientes en la ficha. ¿Qué tipos de datos está tratando la clínica? ¿Qué derechos consagrados en la nueva ley de protección de datos puede ejercer?

La clínica es responsable de tratamiento de datos personales sensibles, específicamente, se trata de datos relativos a la salud y al perfil biológico humano, los que tienen un régimen especial de protección de acuerdo con los artículos, 2 letra g) con la remisión de esta definición del artículo 12 de la Ley 20.584 y del 16 y 16 bis de la ley de protección de datos, como asimismo de forma que estos solo pueden ser tratados para los fines previstos por las

leyes especiales en materia sanitaria, y si no se cuenta con el consentimiento del titular, solo se pueden tratar en los casos especiales señalados en el inciso segundo de la última norma citada.

De esta forma, si la clínica cedió los datos sin el consentimiento del paciente, para fines publicitarios o de marketing, se ha infringido lo dispuesto en el artículo 12 respecto del consentimiento del titular establecido en los artículos 12 y 15, además de los artículos 2 letra g) (artículo 12 de la Ley 20.584), 16 y 16 bis que regulan el tratamiento de los datos sensibles relativos a la salud y perfil biológico de la ley. Por lo tanto, se puede denunciar la infracción a la Agencia de Protección de Datos, aplicando el procedimiento establecido en el artículo 42 de la mencionada ley. La cesión de datos personales sin el consentimiento del titular en los casos que sea necesario o para un fin distinto al autorizado constituye una infracción grave consagrada en la letra b) del artículo 34 ter de la ley, cuya sanción corresponde a una multa superior a 5.000 UTM hasta 10.000 UTM, sin perjuicio de las medidas que la Agencia disponga tendientes a subsanar las causales que dieron motivos a la sanción o de la imposición de sanciones accesorias.

Además, el paciente puede ejercer su *derecho de acceso* consagrado en el artículo 5° de la ley para obtener del responsable confirmación de si sus datos personales han sido cedidos, de acuerdo con lo establecido en la letra c) de la misma norma, es decir, la información sobre las categorías, clases o tipos de destinatarios, o bien, la identidad de cada destinatario, en caso de solicitarlo así el titular, a los que se les hayan comunicado o cedido los datos o se prevea hacerlo.

Respecto de los exámenes antiguos que aparecen como los más recientes, el señor Fuentes puede ejercer el *derecho de rectificación*, para solicitar que se rectifique dicha información.

Si la clínica no responde o no accede a estas solicitudes, puede recurrir a la Agencia de Protección de Datos, a través del procedimiento del artículo 41 de la nueva ley, para el ejercicio de sus derechos.

3. La empresa Consultas Financieras S.A se dedica a ofrecer créditos de consumo en línea. Para ello, recopila datos de sus clientes, específicamente, nombres, cédulas de identidad, domicilios, ingresos, historial crediticio, y además solicita liquidaciones de sueldo. Uno de sus clientes, don Sergio Gutiérrez, les realizó una solicitud exigiendo que eliminen un dato sobre un crédito moroso de hace años, alegando que se pagó hace tiempo y, además, se opone a que sus datos sean utilizados para recibir publicidad de productos financieros, sin embargo, la empresa no respondió la solicitud a tiempo, razón por la que Sergio reclamó ante la Agencia de Protección de Datos Personales. ¿Qué pasos debe seguir la empresa ante este reclamo?

En este caso, el señor Sergio Gutiérrez intentó ejercer sus *derechos de supresión* y *de oposición* a través del procedimiento de los artículos 10 y 11 de la ley. No obstante, la empresa no respondió los requerimientos dentro de los plazos establecidos que consisten en treinta días corridos desde la fecha de ingreso de la solicitud, lo que pude ser prorrogado una vez por otros treinta días corridos.

Dada la falta de respuesta, el titular está facultado para formular una reclamación ante la Agencia, de acuerdo con el procedimiento del artículo 41. Si la Agencia acoge el reclamo a tramitación, notificará a la empresa, quien dispondrá de un plazo de treinta días corridos, prorrogables hasta por el mismo plazo, para responder la reclamación, acompañando todos los antecedentes que estime pertinentes. Luego, la Agencia podrá fijar un término probatorio de diez días, si considera que existen hechos sustanciales, pertinentes y controvertidos. También, la empresa responsable puede allanarse a la reclamación, en cuyo caso deberá acompañar los antecedentes o testimonios que acrediten esta circunstancia, lo que una vez verificado, se le notificará al titular, quien tendrá diez días para hacer valer sus derechos. Cumplido ese plazo, la Agencia procederá al archivo de los antecedentes, previa aplicación de la sanción o instrucción al responsable de datos, cuando corresponda.

La falta de respuesta de la empresa constituye una infracción leve consagrada en la letra c) del artículo 34 bis de la ley, cuya sanción puede corresponder desde una amonestación escrita hasta multa de hasta 5.000 UTM, sin perjuicio de las medidas que la Agencia disponga tendientes a subsanar las causales que dieron motivos a la sanción o de la imposición de sanciones accesorias.

Igualmente, la empresa puede defenderse respecto a la información de la deuda que ya fue pagada con lo dispuesto en el artículo 19 de la ley que consagra que el pago o la extinción de una obligación económica, bancaria o comercia no produce la caducidad o pérdida de fundamento legal de los datos respectivos, mientras esté pendiente el plazo de 5 años desde que la obligación se hizo exigible (consagrado en el artículo anterior). Además, al efectuarse el pago o la extinción de la obligación por otro modo en que intervenga directamente el acreedor, éste tiene el deber de avisar al responsable del registro o base de datos en que su oportunidad comunicó el protesto o la morosidad, de tal hecho a más tardar dentro de los siete días hábiles siguientes, para que se consigne el nuevo dato que corresponda. Esto también puede ser requerido por el propio deudor.

4. **Rosa Castro solicitó a su compañía de telefonía móvil que le dieran acceso a todos sus datos personales que la compañía mantiene, incluyendo nombres, cédula de identidad, historial de llamadas, ubicación georreferenciada, facturaciones, etc.), y que eliminen los registros de ubicación de más de dos años de antigüedad, argumentando que ya no son necesarios para la finalidad original. La empresa entregó una respuesta parcial, con extracto incompleto de los datos y se negó a eliminar los registros de ubicación, argumentando que los necesita para fines comerciales internos. Insatisfecha con la respuesta, recurrió a la Agencia, no obstante, esta estimó que la reclamación no cumplía con todos los requisitos establecidos en el artículo 41 letra a) de la ley, razón por la que no acogió a tramitación el reclamo. ¿Qué puede hacer doña Rosa Castro?**

En conformidad con el artículo 41 letra i) de la ley, la señora Rosa puede impugnar judicialmente la resolución que no acoge a tramitación un reclamo dentro del plazo de quince días hábiles contados desde su notificación, a través de la interposición de un reclamo de ilegalidad ante la Corte de Apelaciones de Santiago o la del lugar donde se encuentre domiciliado el reclamante, a elección de éste, según el procedimiento regulado en el artículo 43 de la ley, donde la Corte podrá confirmar o revocar la resolución impugnada.

5. La empresa "Estudiemos+" administra una plataforma de cursos en línea y, a su vez, es responsable de los datos de miles de estudiantes, incluyendo nombres, cédulas de identidad, correos electrónicos, historiales académicos, notas, resultados de trabajos y/o evaluaciones e incluso datos sensibles como necesidades educativas especiales declaradas por los estudiantes. Un día, el área de sistemas de la empresa detecta que se produjo una filtración de datos que expuso temporalmente nombres y correos electrónicos de algunos estudiantes, los datos sensibles sobre salud o necesidades educativas especiales no se vieron afectados. ¿Qué debería hacer la empresa en relación a los deberes que impone la ley de protección de datos a los responsables del tratamiento de datos?

El responsable de datos tiene el deber de adoptar las medidas de seguridad necesarias para resguardar el cumplimiento del principio de seguridad (artículos y 14 quinquies de la ley de protección de datos), de forma que la filtración señalada constituye una infracción del principio y deber mencionado.

Asimismo, el artículo 14 sexies consagra el deber de reportar las vulneraciones a las medidas de seguridad, de forma que el responsable de datos debe reportar a la Agencia, por los medios más expeditos posibles, las vulneraciones ocurridas, incluyendo expresamente las que ocasionen filtración de datos personales y cuando exista un riesgo razonable para los derechos y libertades de los titulares. Esto cobra mayor importancia si la vulneración afecta datos personales sensibles relativos a niños y niñas menores de catorce años, caso en que la empresa deberá también comunicar a los titulares de estos datos, a través de sus representantes, cuando corresponda. Las infracciones al deber establecido en el artículo 14 quinquies y la omisión de las comunicaciones en casos de vulneración de las medidas de seguridad constituyen infracciones graves establecidas en las letras j) y k) del artículo 34 ter, mientras que la omisión deliberada de la comunicación de las vulneraciones es una infracción gravísima establecida en la letra f) del artículo 34 quáter.

6. José Flores presentó ante la Agencia Nacional de Inteligencia una solicitud de acceso a información pública para obtener la siguiente información: a) Cuántas bases de datos maneja la agencia, b) Bajo qué norma legal se manejan dichas bases de datos y c) Cuáles son esas bases de datos. Esta solicitud fue rechazada arguyendo una excepción al principio de publicidad, al concurrir las causales establecidas en los numerales 3 y 5 del artículo 21 de la Ley 28.285 sobre acceso a la información pública, la última en relación con el artículo 38 de la Ley 19.974. ¿El rechazo a la solicitud por parte de la Agencia Nacional de Inteligencia vulnera alguna de las normas establecidas en la nueva ley de protección de datos?

El artículo 20 de la ley de protección de datos regula el tratamiento de estos por parte de órganos públicos, estableciendo que su tratamiento es lícito, 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. Asimismo, el artículo 23 regula que el titular de los datos puede ejercer ante los órganos públicos los derechos de *acceso, rectificación y oposición* que reconoce la ley e incluso el de *oposición y supresión*. No obstante, la letra b) de la misma norma citada, se menciona que se puede rechazar una solicitud cuando con ello se afecte el carácter secreto de la información establecido por la ley. De esta forma, la discusión se centrará en si la causal de reserva invocada es aplicable. No obstante, nada impide a la Agencia Nacional de Inteligencia informar cuál es la norma legal que le permite almacenar y tratar la información que recopila, pues esta información no es de aquella que se encuentra amparada por el secreto. El no entregar dicha información sí constituye una omisión importante, pues de ello se puede determinar la legalidad del tratamiento de datos por parte de un organismo público, en conformidad al citado artículo 20, sobre todo, ya que, no hay autorización expresa en la ley que habilite a la Agencia Nacional de Inteligencia a recolectar, procesar y comunicar datos personales en el ejercicio de sus funciones. De esta forma, se ha señalado que la Agencia referida no necesita el consentimiento de los titulares de datos que recoja de fuentes abiertas y en el cumplimiento de sus objetivos, o a través de los procedimientos específicos consagrados en la ley para los datos que sean necesarios y que no puedan ser obtenidos de fuentes abiertas[153].

[153] Álvarez y Bordachar (2022:11y siguientes).

7. Francisca Gómez realizó una solicitud al Ministerio Público para eliminar información personal que dicha entidad mantiene en su "Sistema de Apoyo de Fiscales" (SAF), señala que hace tiempo fue parte de un proceso penal que terminó con una sentencia de absolución a su favor. No obstante, sus datos personales quedaron permanentemente registrados en el mencionado sistema. El Ministerio Público se negó a la solicitud, señalando que el SAF no constituye una base de datos, sino que es un respaldo digital de las actividades desarrolladas por la Fiscalía, por lo que no es procedente eliminar nada. ¿Es jurídicamente correcto el rechazo de la solicitud?

Como el Ministerio Público es un organismo público, debemos considerar lo establecido en el artículo 20 de la ley de protección de datos, que regula el tratamiento datos personales por parte de órganos públicos, estableciendo que su tratamiento es lícito, 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. Asimismo, el artículo 23 regula que el titular de los datos puede ejercer ante los órganos públicos los derechos de *acceso, rectificación y oposición* que reconoce la ley e incluso el de *oposición y supresión*.

Así, la letra a) del artículo 7° de la mencionada ley señala expresamente que el titular de datos tiene derecho a solicitar y obtener la eliminación de los datos personales que le concierne cuando los datos no resulten necesarios en relación con los fines del tratamiento para el cual fueron recogidos. Si se considera que la finalidad de la plataforma SAF es el registro de actuaciones para una etapa concreta del procedimiento penal, esto es, la etapa de investigación, y ya no hay ninguna investigación en curso, entonces el fundamento legal que avala el tratamiento de la información personal ha desaparecido, y como la mantención indefinida de datos personales se ha quedado sin propósito, lo que procede es la eliminación o supresión de los mismos, todo esto en concordancia con el principio de finalidad consagrado en la letra b) del artículo 3 de la ley de protección de datos, y de acuerdo con el cual el tratamiento de datos de carácter personal deberá limitarse al cumplimiento de las finalidades determinadas, explícitas y legítimas para el cual fueron recabadas y, por ende, no procede su uso una vez agotada la finalidad[154]. Por lo demás, el artículo 25 establece un régimen especial respecto de los datos relativos a infracciones penales, civiles, administrativas y disciplinarias,

[154] Reusser (2022:70 y siguientes).

indicando que estos solo pueden ser tratados por los organismos públicos para el cumplimiento de sus funciones legales, dentro del ámbito de sus competencias y en los casos expresamente previstos en la ley.

8. Carlos Olave fue condenado por manejo en estado de ebriedad, provocando lesiones a transeúntes. Actualmente, han pasado 10 años desde el día en que salió en libertad luego de cumplir su condena. Un día, navegando por el internet, encontró un blog de crónica roja que contenía una nota del delito que cometió, incluyendo sus datos personales, razón por la que solicitó al motor de búsqueda que elimine toda información personal que afecte su honra y vida privada, debido al fundado temor de que alguien encontrara la nota y fuera despedido o que no pudiera encontrar empleo en el futuro, mencionando expresamente el derecho al olvido y a la pérdida de interés público de la nota debido al tiempo transcurrido desde los hechos. ¿El motor de búsqueda es responsable por el tratamiento de datos personales? ¿Debe acceder a la solicitud realizada por el señor Carlos Olave?

Existe una tendencia a determinar que los motores de búsqueda no tienen legitimidad pasiva para ser recurridos por vulneraciones a los derechos a la honra o a la vida privada puesto que el acto que produce la afectación eventual de estos derechos es efectuado por un tercero, por quien el motor de búsqueda no responde. No obstante, se discute la extensión de esta eximición de responsabilidad ya que pareciera ser demasiado amplia. Con todo, lo determinante es si es posible clasificar a los motores de búsquedas como responsables del tratamiento de datos personales, pues de ser así, le resultarían aplicables las disposiciones de la nueva Ley 19.628 y, por ende, debería acoger a tramitación la solicitud realizada por el señor Olave de acuerdo con los procedimientos, derechos y deberes establecidos en la mencionada ley. De lo contrario, el titular de datos no podrá dirigirse en su contra, sino que deberá accionar en contra de cada uno de los titulares de los sitios web en donde se encuentre dicha información[155].

[155] Arancibia (2022:73-88).

9. Catalina Rodríguez terminó sus estudios universitarios en 2009. Para financiarlos, solicitó un crédito complementario al Fondo Solidario. En el año 2015 se inició un proceso ejecutivo para el cobro de dicho crédito, sin embargo, se alegó que tales obligaciones se encontraban prescritas, dictándose sentencia que acogió dicha excepción. No obstante, al solicitar su informe de deudas, la referida deuda declarada judicialmente prescrita estaba incluida como una deuda vigente. ¿La empresa a cargo del informe de deudas ha incurrido en alguna infracción a la nueva ley de protección de datos personales?

El artículo 17, inciso segundo, señala que no podrá comunicarse la información relacionada con las deudas contraídas con instituciones de educación superior de conformidad a las leyes números 18.591 y 19.287, ni aquellas adquiridas con bancos o instituciones financieras de conformidad a la Ley 20.027, o en el marco de las líneas de financiamiento a estudiantes para cursar estudios en educación superior, administradas por la Corporación de Fomento de la Producción, ni alguna deuda contraída con la finalidad de recibir para sí o para terceros un servicio educacional formal en cualquiera de sus niveles. A su vez, el artículo 18 de la misma ley señala que no podrán comunicarse los datos a que se refiere el artículo anterior, que se relacionen con una persona identificada o identificable, luego de transcurridos cinco años desde que la respectiva obligación se hizo exigible. Por último, el inciso final del artículo 19 señala que la infracción de cualquiera de estas obligaciones se conocerá y sancionará de conformidad a lo dispuesto en el Título VII de esta ley, de forma que, considerando todas estas normativas, la información sobre la deuda contraída por Catalina para financiar sus estudios y que fue declarada prescrita por una sentencia judicial no debía incluirse en su informe de deudas, de forma que la empresa infringió la normativa señalada.

10. Durante el año 2020, en el contexto de la pandemia de COVID-19, el Ministerio de Salud solicitó a la Contraloría que emitiera pronunciamiento sobre si era procedente o no la comunicación de datos sensibles a las municipalidades, en específico, el diagnóstico de pacientes COVID-19 positivos. La Contraloría, en el dictamen N°8.113 de 2020 determinó dicha información forma parte de la ficha clínica de los pacientes y, en consecuencia, constituye un dato sensible, sujeto a reserva de acuerdo con lo dispuesto en el artículo 12 de la Ley 20.584. Considera, además, que el Ministerio de Salud puede acceder a dicha información de acuerdo con lo dispuesto en el Reglamento N°41 de 2012, del Ministerio de Salud y al N°5 del artículo 4 del Decreto con Fuerza de Ley N°1 de 2006. No obstante, determina que las municipalidades no pueden acceder a dicha información por sus propias facultades, de forma que tampoco podría acceder a ella de forma indirecta, por lo que el Ministerio no podría comunicarla. La excepción es que el propio paciente, titular de la información, consienta en su comunicación y tratamiento. ¿El criterio sería el mismo en conformidad con la nueva ley de protección de datos?

La ley de protección de datos incorpora el artículo 22, que regula la comunicación o cesión de datos por parte de un órgano público, estableciendo que estos están facultados para comunicar o ceder datos personales específicos, o todo o parte de sus bases de datos o conjuntos de datos, a otros órganos públicos, siempre que la comunicación o cesión de los datos resulte necesaria para el cumplimiento de sus funciones legales y ambos órganos actúen dentro del ámbito de sus competencias. La comunicación o cesión de los datos se debe realizar para un tratamiento específico y el órgano público receptor no los podrá utilizar para otros fines. Con todo, esta normativa no modifica el criterio de la Contraloría, por cuanto no modifica las funciones o facultades de las municipalidades para acceder a estos datos.

No obstante, la ley ahora también incorpora el artículo 16 bis que regula el tratamiento de datos personales sensibles relativos a la salud y perfil biológico humano que, faculta el tratamiento de este tipo de datos, sin el consentimiento del titular, en los casos que enumera, siendo el establecido en la letra b) en casos de alerta sanitaria legalmente decretada, norma que sí afectaría el criterio del dictamen de Contraloría, por cuanto la alerta sanitaria decretada por la pandemia de COVID-19 podría haber permitido que la municipalidad

tratara dichos datos sensibles sin el consentimiento de su titular, el que, en otras circunstancias, habría sido necesario.

11. Elena Alvarado es una adulta mayor de 68 años. Hace unos días, sufrió un episodio de descompensación debido a que es diabética, razón por la que fue socorrida por el Sistema de Atención Médica de Urgencia -SAMU-. La señora Elena vive sola y además sufre de demencia, de forma que no fue capaz de proporcionar los datos necesarios sobre su identidad al personal de salud, por esa razón, se procedió a identificarla a través de su huella dactilar. ¿Es correcto este procedimiento en conformidad con la nueva normativa de protección de datos?

Se ha estimado que los datos de identidad de la persona no son datos sensibles, sino datos provenientes de una fuente accesible al público y que la identificación de pacientes es un proceso esencial en la realización de las acciones y prestaciones de salud, que permite el correcto registro de dichas acciones en la ficha clínica, de forma que a estos datos podrían acceder todos los funcionarios que participan en cada una de las etapas del proceso y no solo aquellos que intervienen directamente en el otorgamiento de las prestaciones de salud[156].

El artículo 16 ter, introducido en la nueva normativa, regula expresamente el tratamiento de los datos biométricos. En su inciso final, señala que estos datos podrán tratarse sin consentimiento sólo en los casos señalados en el inciso segundo del artículo 16 bis, entre los cuales se encuentra establecido en la letra a) cuando resulte indispensable para salvaguardar la vida o integridad física o psíquica del titular o de otra persona o, cuando el titular se encuentre física o jurídicamente impedido de otorgar su consentimiento. Una vez que cese el impedimento, el responsable debe informar detalladamente al titular los datos que fueron tratados y las operaciones específicas de tratamiento que fueron realizadas. Si bien la normativa señalada no legitima el uso de estos datos para la finalidad de identificación del paciente, puede abrir una puerta para autorizar el tratamiento de estos datos cuando el paciente, por su propio estado de salud, no puede consentir u otorgar la información necesaria para su identificación, etapa que es fundamental para que el paciente reciba una adecuada atención de salud.

[156] Donoso (2022:172 y siguientes).

12. Martín Salgado es el representante legal de una empresa que se dedica a la compra y venta de verduras y productos agrícolas. No obstante, en el año 2015, sufrió problemas económicos que lo llevaron a tener varias facturas impagas que fueron publicadas en su informe de deudas. Actualmente, solicitó a la empresa que gestiona los informes de deudas y se percató de que las facturas siguen apareciendo, pese a que por el tiempo transcurrido ya están prescritas, por ello, solicitó que se elimine dicha información del informe de deudas, amparándose en la ley de protección de datos. ¿Puede la empresa agrícola ejercer los derechos que otorga la ley de protección de datos?

La Ley 19.628 define, en su artículo 2 letra f) que dato personal como cualquier información vinculada o referida a una *persona natural* identificada o identificable, asimismo, en la letra ñ) se define al titular de datos como la *persona natural*, identificada o identificable, a quien concierne o se refieren los datos personales. Además, en el artículo 1° de la ley al definir el objeto y ámbito de aplicación se señala que el objeto de la ley es regular la forma y condiciones en la cual se efectúa el tratamiento y protección de los datos personales de las *personas naturales*. De esta forma, la ley solamente protege y ampara los datos personales de las personas naturales, excluyendo a las personas jurídicas de su ámbito de aplicación, por tanto, la empresa de Martín no puede ejercer los derechos regulados en esta ley. Así, también, lo ha señado la jurisprudencia.[157]

[157] Corte Suprema, Conectados S.A. con Empresa Nacional de Comunicaciones S.A. y otros, rol 11627-2014, 31 de julio de 2014.

13. Cristóbal Martínez lleva trabajando más de 10 años para la misma empresa. En el último tiempo, fue diagnosticado con una enfermedad crónica que disminuye su capacidad física, de forma que lo notificó a su empleador y se ha mantenido realizando solo labores de escritorio. No obstante, hace unos días, su empleador respondió un correo electrónico con una consulta de uno de sus compañeros, dirigiéndolo a todos los empleados de la empresa. En dicha comunicación, se mencionaba el diagnóstico de Cristóbal que lo mantenía exclusivamente con labores de escritorio. ¿Se ha afectado el derecho a la protección de datos personales de Cristóbal? ¿Qué puede realizar?

El empleador de Cristóbal ha infringido el deber de secreto o confidencialidad consagrado en el artículo 14 bis de la nueva ley de protección de datos, que lo obliga a mantener secreto o confidencialidad acerca de los datos personales que conciernen a un trabajador. Con ello, también se ha infringido el principio de seguridad establecido en la letra f) del artículo 3° y el principio de confidencialidad establecido en la letra h) de la misma norma. Esta infracción adquiere mayor relevancia si consideramos que la información compartida corresponde a un dato personal sensible relativos a la salud y al perfil biológico humano. La vulneración del deber de secreto o confidencialidad es una infracción grave consagrada en la letra i) del artículo 34 ter mientras que vulnerar este mismo deber sobre datos personales sensibles constituye una infracción gravísima establecida en la letra d) del artículo 34 quáter. Por ello, Martín puede presentar una reclamación ante la Agencia siguiendo el procedimiento establecido en el artículo 42 y, además, el empleador es también responsable civilmente de indemnizar el daño patrimonial y extrapatrimonial que haya causado con su infracción a los principios y obligaciones establecidos en la ley, de conformidad al artículo 47.

14. Sofía Fuentes es madre de dos niños menores de edad y actualmente está pasando por proceso de divorcio complicado y se está discutiendo el cuidado personal de los niños con su marido. En dicho proceso, su marido solicitó que se oficiará a la clínica privada en donde Sofía se atiende siempre, para que remita su ficha clínica, incluyendo las atenciones que ha realizado, los diagnósticos, exámenes y medicamentos indicados. La clínica cumplió con el oficio y acompañó a la causa la ficha clínica completa de Sofía, la que incluía información muy sensible como las declaraciones de ella realizadas a profesionales de la salud respecto de su familia, problemas de autoestima e incluso sus sentimientos sobre el matrimonio, relatando incluso los encuentros con su psiquiatra, haciendo publica dicha información no solo a su marido, al tribunal y a los abogados, sino que también a terceros. ¿Qué derechos consagrados en la nueva ley de protección de datos han sido vulnerados?

El artículo 12 de la Ley 19.628 dispone que el tratamiento de los datos personales que conciernen al título es lícito cuando éste otorgue su consentimiento para ello, de forma que el consentimiento debe ser libre, informado y específico en cuanto a su finalidad o finalidades. De esta forma, el responsable de datos solo puede realizar el tratamiento para los fines específicos respecto de los que el titular haya consentido, conforme a los principios de licitud y lealtad y de finalidad establecidos en las letras a) y b) del artículo 3°. Así, la clínica en primer lugar ha transgredido el artículo12 y 13 de la Ley N° 20.584 respecto a los datos sensibles que se contienen en la ficha clínica de un paciente. Esta infracción adquiere mayor relevancia si consideramos que la información compartida corresponde a un dato personal sensible relativos a la salud y al perfil biológico humano. Además, ha infringido el deber de secreto o confidencialidad consagrado en el artículo 14 bis de la ley de protección de datos, que lo obliga a mantener secreto o confidencialidad acerca de los datos personales que conciernen a un titular. Con ello, también se ha infringido el principio de seguridad establecido en la letra f) del artículo 3° y el principio de confidencialidad establecido en la letra h) de la misma norma. La vulneración del deber de secreto o confidencialidad es una infracción grave consagrada en la letra i) del artículo 34 ter mientras que vulnerar este mismo deber sobre datos personales sensibles constituye una infracción gravísima establecida en la letra d) del artículo 34 quáter. Por ello, la clínica podría enfrentarse a un procedimiento infraccional ante la Agencia de Protección de Datos de acuerdo con el artículo 42 y, además,

también es responsable civilmente de indemnizar el daño patrimonial y extrapatrimonial que haya causado con su infracción a los principios y obligaciones establecidos en la ley, de conformidad al artículo 47 y las reglas generales de responsabilidad. El hecho de la que la clínica haya actuado en cumplimiento de una orden judicial, emitiendo la información oficiada, no impide ni cambia las vulneraciones mencionadas, especialmente, porque la clínica no se limitó a enviar la información solicitada en el oficio, sino que compartió la ficha clínica completa. Este criterio ha sido sostenido por la Corte de Apelaciones de Santiago en vigencia de la antigua ley, no habiendo motivos para que este criterio cambie con la nueva ley.[158]

15. EYESCOIN S.A. es una empresa que se dedica al tratamiento de datos y que inició una campaña de recolección de datos biométricos, ofreciendo a los voluntarios que estén dispuestos a entregar sus datos biométricos, específicamente, su iris, una compensación en criptomonedas. Marcelo Rojas Véliz, tiene 14 años y vio el anuncio de EYESCOIN S.A., ante la propuesta de conseguir dinero fácil en criptomonedas, decidió participar de la campaña y, con fecha 30 de enero de 2025, entregó los datos biométricos de su iris a cambio de criptomonedas. Cuando los padres de Marcelo, Valeria Véliz y Raúl Rojas, se enteraron de cómo su hijo había conseguido las criptomonedas y manifestaron claramente su desacuerdo y preocupación de que una empresa desconocida tenga los datos biométricos de su hijo, al cuestionarle que haría la empresa con los datos o para qué los quería, Marcelo dijo que no tenía idea, no preguntó y tampoco se lo informaron. Por ello, Valeria y Raúl intentaron contactarse con la empresa para solicitar la eliminación de los datos de su hijo, que fueron obtenidos sin que él pueda consentir derechamente pues se trata de un menor de edad y, evidentemente, no se solicitó autorización a sus progenitores, sin embargo, pese a sus numerosos intentos no han recibido respuesta. ¿Qué normas se han infringido en este caso?

En este caso se involucran datos sensibles, específicamente, datos personales biométricos cuyo tratamiento está consagrado en el artículo 16 ter, donde se señala que el responsable debe proporcionar al titular la identificación

[158] Corte de Apelaciones de Santiago, *González López con Clínica Alemana de Santiago*, rol 11030-2015, 21 de diciembre de 2015 y 20° Juzgado Civil de Santiago, *González López con Clínica Alemana de Santiago,* rol C-20968-2014, 11 de septiembre de 2015.

del sistema biométrico usado, la finalidad específica para la cual los datos recolectados por el sistema biométrico serán utilizados, el periodo durante el cual los datos biométricos serán utilizados y la forma en que el titular puede ejercer sus derechos.

Igualmente, estamos ante una categoría especial de datos personales, esto es, a datos personales relativos a los NNA, cuyo tratamiento está regulado en el artículo 16 quáter. Así, como se trata de datos sensibles, al tratarse de un menor de 16 años, se requiere el consentimiento otorgado por sus padres o representantes legales o quien tiene a su cargo el cuidado personal del menor, de forma que no basta el consentimiento del niño menor de 14 años, es más, quien solo puede consentir para el tratamiento de datos personales no sensibles.

La empresa, además, ha infringido el deber de información y transparencia al no informar al titular sobre las categorías, clases o tipos de datos que trata; la descripción genérica del universo de personas que comprenden sus bases de datos; los destinatarios a los que se prevé comunicar o ceder los datos; las finalidades de los tratamientos que realiza; la base de legitimidad del tratamiento; y en caso de tratamientos que se basan en la satisfacción de intereses legítimos, cuáles serían éstos, la política y las medidas de seguridad adoptadas para proteger las bases de datos personales que administra, el periodo durante el que se conservarán los datos personales, todo de conformidad al artículo 14 ter de la Ley 19.628.

La infracción al deber de información y transparencia y la omisión de la respuesta a las solicitudes formuladas por el titular de datos o por su representante, constituyen infracciones leves establecidas en el artículo 34 bis letras a) y c), respectivamente. Por su parte, el tratamiento de datos personales sin el consentimiento del titular, y realizar el tratamiento de datos personales de niños, niñas y adolescentes con infracción a las normas previstas en la ley constituyen infracciones graves consagradas en el artículo 34 ter letras a) y g). Por último, tratar datos personales sensibles de niños, niñas y adolescentes en contravención a las normas de esta ley constituye una infracción gravísima establecida en el artículo 34 quáter letra e). Por ello, la empresa podría enfrentarse a un procedimiento infraccional ante la Agencia de Protección de Datos de acuerdo con el artículo 42 y, además, también es responsable civilmente de indemnizar el daño patrimonial y extrapatrimonial que haya causado con su infracción a los principios y obligaciones establecidos en la ley, de conformidad al artículo 47.

BIBLIOGRAFÍA

Acedo Penco, Ángel y Platero Alcón, Alejandro (2016). "La privacidad de los niños y adolescentes en las redes sociales: Referencia especial al régimen normativo europeo y español, con algunas consideraciones sobre el chileno". *Revista Chilena de Derecho y Tecnología*, 5, (1): 63–94. DOI: 10.5354/0719-2584.2016.42557.

Alexy, Robert (1983). *Teoría de los Derechos Fundamentales*. Madrid: Centro de Estudios Constitucionales.

Álvarez Escudero, Rommy (2020). "Los derechos de la personalidad de niños, niñas y adolescentes en el entorno digital". En Judith Solé y Vinicius Almada (coordinadores) *Protección de los menores de edad en la era digital* (52 –72) Porto: Editorial Juruá.

Álvarez Escudero, Rommy y Prado López, Pamela (2023). *Derechos de la personalidad, derechos fundamentales y responsabilidad civil. Cuestiones relevantes*. Ciudad de México: Tirant lo Blanch.

Álvarez Escudero, Rommy y Riveros Ferrada, Carolina (2025). "Derecho a la autodeterminación y derechos de la personalidad de niños, niñas y adolescentes en sus atenciones de salud en Chile"». *Revista de Derecho Privado*, 49: 85–110. DOI: 10.18601/01234366.49.03

Álvarez Valenzuela, Daniel y Bordachar Benoit Michelle (2022). "Comentario a la sentencia Rol N°29507-2019 de la Excelentísima Corte Suprema". En Pablo Conteras, Michelle Bordachar y Leonardo Ortis (editores), *Privacidad y protección de datos personales. Jurisprudencia seleccionada y comentada* (pp.3-18). Santiago: DER Ediciones.

Arancibia Obrador, María José (2022). "Comentario a las sentencias Roles N°s. 54-2020, 20726-2020, 31815-2020 y 41260-2020 de la Excelentísima Corte Suprema". En Pablo Contreras, Michelle Bordachar y Leonardo Ortis (editores), *Privacidad y protección de datos personales. Jurisprudencia seleccionada y comentada* (pp.73-88). Santiago: DER Ediciones.

Arenas Massa, Ángela (2023). "La convención interamericana sobre protección de los derechos humanos de las personas mayores y su posible proyección hacia una convención internacional". En Carolina Riveros, Alexis Mondaca, Isaac Ravetllat (edits). *Derecho y Grupos en situación de vulnerabilidad social: Personas mayores, inmigrantes, niños, niñas y adolescentes y personas de género diverso* (pp.13-31). Valencia: Tirant Lo Blanch.

Ayres, Ian y Braithwaite, John (1992). *Responsive Regulation: Transcending the Deregulation Debate*. Oxford: Oxford University Press.

Barranco Avilés, María del Carmen (2025). "La carta española de derechos digitales y los derechos humanos de los niños, niñas y adolescentes". *Revista de Derecho Privado*, 48: 47–68. DOI: 10.18601/01234366.48.03

Barros Bourie, Enrique (2010). *Tratado de la responsabilidad civil extracontractual*. Santiago: Editorial Jurídica de Chile.

Bassi Díaz, Francisco (2017). "Culpa infraccional. Elementos para una perspectiva crítica sobre sus efectos jurídicos en el derecho civil chileno". *Revista de Estudios de la Justicia*, 27: 37- 59. DOI: 10.5354/0718-4735.2017.47960

Bennett, Colin J., y Raab, Charles D. (2006). *The Governance of Privacy: Policy Instruments in Global Perspective*. Cambridge: MIT Press.

Bermúdez Soto, Jorge (2018). *Derecho Administrativo General*. Santiago: Legal Publishing, Santiago.

Biblioteca del Congreso Nacional (2024). *Historia de la Ley N°21.719*. Disponible en https://www.bcn.cl/historiadelaley/nc/historia-de-la-ley/8352/, fecha de consulta: 19 de enero de 2026.

Bioni, Bruno Ricardo (2019). *Proteção de dados pessoais: a função e os limites do consentimiento.* Rio de Janeiro: Forense.

Black, Julia (2002). "Critical Reflections on Regulation". *Australian Journal of Legal Philosophy* 27: 1–10 (esp. 6–9).

Bygrave, Lee A. (2002). *Data Protection Law: Approaching Its Rationale, Logic and Limits*. Oxford: Oxford University Press.

Campos Rivera, Gonzalo (2024). "Credit scoring como tratamiento de datos personales a la luz del RGPD: análisis de su finalidad e influencia en los posibles usos secundarios de los datos". *Revista de Derecho UNED* (33): 111 ss. (PDF provisto en el Proyecto).

Cappelletti, Mauro y Garth, Bryant (1978). *Access to Justice*, Vol. I. Leiden: Sijthoff.

Casadei, Thomas (2025). "Regulation, Awareness, Agency: Beyond the "Risk Paradigm"". *Revista de Derecho Privado*, 48: 5–18. DOI: 10.18601/01234366.48.01.

Cassagne, Juan Carlos (2011). *Derecho Administrativo*. Buenos Aires: Abeledo Perrot, Buenos Aires.

Cavaller Vergés, Misericordia (2024). "El concepto autónomo de responsabilidad civil en el ámbito de la protección de datos personales en la era digital: Análisis del artículo 82 del Reglamento 2016/679". *Revista de Derecho Comunitario Europeo*, 79: 251 – 292. DOI: 10.18042/cepc/rdce.79.09.

CNIL (2018). «Règlement européen sur la protection des données — Chapitre II: Principes». *Commission nationale de l'informatique et des libertés*. Disponible en https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre2, fecha de consulta: 19 de enero de 2026.

Comité de los Derechos del Niño (2021). *Observación General N°25 relativa a los derechos de los niños en relación con el entorno digital*. Disponible en: https://docs.un.org/es/CRC/C/GC/25, fecha de consulta: 19 de enero de 2026.

Comité Europeo de Protección de Datos (2025). *Declaración 1/2025 sobre la determinación de la edad*. Disponible en https://www.edpb.europa.eu/system/files/2025-07/edpb_statement_20250211ageassurance_es.pdf, fecha de consulta: 19 de enero de 2026.

Contreras Vásquez, Pablo y Trigo Kramcsák, Pablo (2019). "Interés legítimo y tratamiento de datos personales: antecedentes comparados y regulación en Chile". *Revista Chilena de Derecho y Tecnología*, 8(1): 69–106. DOI: 10.5354/0719-2584.2019.52915.

Contreras Vásquez, Pablo (2020). "El derecho a la protección de datos personales y el reconocimiento de la autodeterminación informativa en la Constitución chilena". *Estudios Constitucionales,* 18(2): 87-120. DOI: 10.4067/S0718-52002020000200087

Contreras, Pablo, Marcelo Drago y Pablo Viollier (2025). *Compliance y protección de datos personales. Explicación de la nueva ley N°21.719*. Santiago: DER Ediciones.

Copello, Nadia (2022). "Manuela, víctima de los estereotipos de género". UBP. Revista Derecho y Salud, Año 6, NÚM, 7, 97-106. DOI: 10.37767/2591-3476 (2022)06 .

Cordero Vega, Luis (2019). *Derecho Administrativo Sancionador*. Santiago: Thomson Reuters.

Corral Talciani, Hernán (2004). *Lecciones de Responsabilidad Civil Extracontractual*. Santiago: Editorial jurídica de Chile.

De Ángel Yágüez, Ricardo (1993). *La prueba del daño*. Madrid: Civitas.

De Hert, Paul y Gutwirth, Serge (2009). "Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action". En Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile Terwangne, Sjaak Nouwt, (eds) *Reinventing Data Protection?* (pp. 3-44). Springer: Dordrecht. https://doi.org/10.1007/978-1-4020-9498-9_1

De Hert, Paul y Papakonstantinou, Vagelis (2016). "The new General Data Protection Regulation: Still a sound system for the protection of individuals?". *Computer Law & Security Review*, 32 (2): 185–188.

Defensoría de la Niñez de Chile (2024). *Documento especializado violencia sexual digital contra niños, niñas y adolescentes.* Disponible en https://www.defensorianinez.cl/wp-content/uploads/2024/12/ESPECIALIZADO-VIOLENCIA-DIGITAL-FINAL.pdf, fecha de consulta: 19 de enero de 2026.

Doneda, Danilo y Mendes, Laura Schertel (2014). *Privacidade, proteção de dados e defesa do consumidor.* São Paulo: Revista dos Tribunais.

Doneda, Danilo (2006). *Da privacidade à proteção de dados pessoais.* Río de Janeiro: Renovar.

Donoso Abarca, Lorena (2022). "Comentario al Dictamen N°009545N20 de la Contraloría General de la República". En Pablo Conteras, Michelle Bordachar y Leonardo Ortis (editores), *Privacidad y protección de datos personales. Jurisprudencia seleccionada y comentada* (pp.169-180). Santiago: DER Ediciones.

Donoso Abarca, Lorena y Reusser Monsálvez, Carlos (2021). "Protección de Datos Personales". *Colección Materiales Docentes N°32 Academia Judicial de Chile.* Disponible en https://academiajudicial.cl/wp-content/uploads/2022/03/Proteccion-de-Datos-personales.pdf, fecha de consulta: 16 de enero de 2026.

Dworkin, Ronald (1989). *Los derechos en Serio.* Barcelona: Ariel.

Egusquiza Balmaseda, María Ángeles (2025). "Protección de datos de salud y responsabilidad civil: Algunos apuntes comparados entre España y Perú". *Actualidad Jurídica Iberoamericana*, 22: 176 – 219.

Estepa Montero, Manuel (2022). "El principio de responsabilidad proactiva o rendición de cuentas como informador del régimen jurídico de la protección de datos de las personas físicas". *Anuario Jurídico y Económico Escurialense*, LV: 67–90.

Esteve Pardo, José (2009). *El desconcierto del Leviatán. Política y derecho ante las incertidumbres de la ciencia.* Madrid: Marcial Pons.

Estrada Vásquez, Francisco y Valenzuela Rivera, Esther (2023), "Ley 21.430 sobre garantías y protección integral de los derechos de la niñez y adolescencia". *Colección Materiales Docentes N°67 Academia Judicial de Chile.* Disponible en: https://academiajudicial.cl/wp-content/uploads/2024/02/MD67-Ley-21430-sobre-garantias-y-proteccion-integral-de-los-derechos-de-la-ninez-y-adolescencia.pdf, fecha de consulta: 19 de enero de 2019.

Fix-Zamudio, Héctor (2005). *Derecho procesal constitucional.* Ciudad de México: UNAM.

Floridi, Luciano (2013). *The Ethics of Information.* Oxford: Oxford University Press.

FRA, TEDH, Consejo de Europa y SEPD (2018). *Handbook on European data protection law.* Luxembourg: Publications Office of the European Union.

Garante per la protezione dei dati personali (2018). *Principi fondamentali del trattamento (art. 5 GDPR).* Disponible en https://www.gdpr-privacy-2018.it/gdpr-privacy-come-funziona/gdpr-principi-fondamentali-introdotti/#:~:text=I%20principi%20fondamentali%20introdotti%20dal%20GDPR%20sono%3A%20liceit%C3%A0%2C,trasparenza%2C%20limitazione%20e%20minimizzazione%2C%20esattezza%2C%20integrit%C3%A0%20e%20riservatezza, fecha de consulta: 19 de enero de 2026.

García de Enterría, Eduardo y Fernández, Tomás-Ramón (2011). *Curso de Derecho Administrativo*, Vol. II. Madrid: Civitas.

Garrido Iglesias, Romina y Sáenz López, Benjamín (2024). *Ley de Protección de Datos Personales: Aspectos claves y desafíos.* Santiago: DER Ediciones.

Gil Antón, Ana (2013). "La privacidad del menor en internet". *Revista de Derecho, Empresa y Sociedad*, 3: 60-96.

Gómez de la Torre Vargas, Maricruz (2018). "La implicancia de considerar al niño sujeto de derechos". *Revista de Derecho UCUDAL*, 18 (14): 117–137. DOI: 10.22235.rd.v18i2.1703

González Fuster, Gloria (2014). *The Emergence of Personal Data Protection as a Fundamental Right of the EU.* Dordrecht: Springer. https://doi.org/10.1093/idpl/ipu034

Guzmán Vega, Nicolás (2025). "Datos personales del trabajador y protección de la privacidad e intimidad, peligros latentes y tareas pendientes". En Guzmán Vega, Nicolás y Verdugo Jaña, Francisco, *La protección y el tratamiento de datos personales* (pp. 23- 43) Santiago: Editorial Hammurabi.

Huergo Lora, Alejandro (2007). *Las sanciones administrativas*. Madrid: Iustel.

Ibáñez Meza, Nicolas (2023). "Concepto moderno de daño en la responsabilidad civil y algunas reflexiones sobre su aplicación en el contexto del uso de entornos virtuales por niños y adolescentes". En Ruperto Pinochet (director), *Estudios de Derecho Civil XVI* (pp. 913–931). Santiago: Thomson Reuters.

IHK Rhein-Neckar (2025). "Die Grundsätze der Datenverarbeitung (Art. 5 Abs. 1 DSGVO)". *Industrie- und Handelskammer Rhein-Neckar* (guía informativa). Disponible en https://www.ihk.de/rhein-neckar/recht/datenschutz-itrecht-internetrecht/datenschutz/grundsaetze-datenverarbeitung-4554126, fecha de consulta: 19 de enero de 2026.

Jijena Leiva, Renato (2025). "Ciberseguridad y Protección de datos personales: la importancia de los estándares iso 27001 y ss". *Actualidad Jurídica* n.° 52 - Julio 2025: 201-230.

Kerr, Orin S. (2004). "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution". Michigan Law Review, 102: 801-888. https://doi.org/10.2307/4141982

Kuner, Christopher (2007). *European Data Protection Law: Corporate Compliance and Regulation*. Oxford: Oxford University Press.

Larenz, Karl (2001). *Metodología de la ciencia del derecho*. Barcelona: Ariel.

León Correa, Francisco (2012). "Información y consentimiento informado de menores de edad en Chile". *Revista chilena de Pediatría*, 83 (2): 113-116. DOI: 10.4067/S0370-41062012000200001.

Lorente López, María (2015). "La vulneración del derecho al honor, a la intimidad y a la propia imagen de los menores a través de las nuevas tecnologías". *Revista Aranzadi Doctrinal*, 2: 207 – 222.

Lynskey, Orla (2015). *The Foundations of EU Data Protection Law*. Oxford: Oxford University Press

Martínez Vásquez de Castro, Luis (2020). "Consentimiento del menor, protección de datos y redes sociales". En Judith Sole y Vinícius Almada (coords), *Protección de los menores de edad en la era digital* (223 – 247). Porto: Editorial Juruá.

Mashaw, Jerry L. (1983). *Bureaucratic Justice*. New Haven: Yale University Press.

Mendes, Laura Schertel (2020). *Privacidade, proteção de dados e defesa do consumidor*, 2ª ed. São Paulo: Thomson Reuters Brasil.

Müller, Guzmán Karl (2021). "Antecedentes sobre la relevancia de los derechos humanos de las personas mayores en la Comunidad Internacional y de su regulación en el Derecho Internacional e interamericano". En Carolina Riveros (ed.). *Protección Jurídica de las personas mayores en Chile* (pp.45-69). Valencia: Tirant Lo Blanch.

Nieto, Alejandro (2012). *Derecho Administrativo Sancionador*. Madrid: Tecnos.

Nogueira Alcalá, Humberto (2010). *Derechos fundamentales y garantías constitucionales*, Tomo II. Santiago: Librotecnia.

OECD (2014). *Regulatory Enforcement and Inspections*. París: OECD Publishing.

OECD (2015). *The Governance of Regulators*, OECD Publishing, París, pp. 15–22 y 73–77.

Ordóñez Pineda, Luis y Calva Jiménez, Stefany (2020). "Amenazas a la privacidad de los menores de edad a partir del sharenting". *Revista Chilena de Derecho y Tecnología*, 9 (2):105-130. DOI: 10.5354/0719-2584.2020.55333.

Ornelas, Lina (2010). "El derecho de las niñas, niños y adolescentes a la protección de sus datos personales: Evolución de derechos y su exigencia frente a las redes sociales". En Instituto Federal de Acceso a la Información y Protección de Datos, *Protección de datos personales* (pp.154–186). México DF: Tiro Corto Editores.

Parra Sepúlveda, Darío y Ravetllat Ballesté, Isaac (2019). "El consentimiento informado de las personas menores de edad en el ámbito de la salud". *Ius et Praxis*, 25 (3), 215-248. DOI: 10.4067/S0718-00122019000300215.

Parra Sepúlveda, Darío y Ravetllat Ballesté, Isaac (2023). "El consentimiento informado de niñas, niños y adolescentes". En Alexis Mondaca, Alejandra Illanes e Isaac Ravetllat (coordinadores), *Lecciones de Derecho de Infancia y Adolescencia II* (pp. 69–91). Valencia: Tirant lo Blanch.

Pérez Luño, Antonio-Enrique (2018). *Derechos Humanos, Estado de Derecho y Constitución*. Madrid: Tecnos.

Pino, Francisco (2025). *Nuevas tendencias regulatorias: Tratamiento y Protección de Datos Personales en Chile. Esquema y comentarios prospectivos*. Santiago: Rubicón, Editores.

Ravetllat Ballesté, Isaac y Basoalto Riveros, Constanza (2021). "La protección de datos personales de niños, niñas y adolescentes: respuestas desde el ordenamiento jurídico chileno". *Estudios Constitucionales*, 19 (1): 111-145. DOI: 10.4067/S0718-52002021000100111.

Reusser Monsálvez, Carlos (2021). *Derecho al olvido. La protección de datos personales como límites a las libertades informativas.* Segunda edición actualizada y complementada. Santiago: DER, Ediciones.

Reusser Monsálvez, Carlos (2022). "Comentario a las sentencias Roles N°s. 25753-2019, 31861-2019,1440-2020 y 76378-2020 de la Excelentísima Corte Suprema". En Pablo Conteras, Michelle Bordachar y Leonardo Ortis (editores), *Privacidad y protección de datos personales. Jurisprudencia seleccionada y comentada* (pp.61-72). Santiago: DER Ediciones.

Riefa, Christine. (2022). "Protecting vulnerable consumers in the digital single market". *European Business Law Review*, 33(4): 541-572.

Riveros, Carolina, Moraga, Claudia y Arenas Ángela (En imprenta). "The Impact of Obstetric Violence on Women's privacy and Data Health Rights: The Inter-American Court of Human Rights Ruling in the Case of Manuela* et al. v. El Salvador". *Revista Dike, Irene y Eunomia.*

Riveros Ferrada, Carolina y Arratia Rojas, Paulina (2025). "El derecho a la propia imagen del paciente en el sistema jurídico chileno". *Revista Chilena de Derecho*, 52 (1): 5 – 66. DOI: 10.7764/R.512.2.

Riveros Ferrada, Carolina y López Díaz, Patricia (2025). "Grupos vulnerables y tutela civil en la nueva regulación de protección de datos en Chile". *Jurídicas CUC*, 21 (1): 261 – 288. DOI: 10.17981/juridcuc.21.1.2025.14.

Rouvroy, Antoinette y Poullet, Yves (2009). "The right to informational self-determination and the value of self-development: reassessing the importance of privacy for democracy". En *Reinventing Data Protection: Proceedings of the International Conference* (Brussels, 12-13 October 2007) (pp.45-76). Springer: Dordrecht.

Rubí Puig, Antoni (2018). "Daños por infracciones del derecho a la protección de datos personales. El remedio indemnizatorio del artículo 82 RGPD". *Revista de Derecho Civil*, V, (4): 53-87.

Rubí Puig, Antoni (2019). "Problemas de coordinación y compatibilidad entre la acción indemnizatoria del artículo 82 del reglamento general de protección de datos y otras acciones en derecho español". *Derecho Privado y Constitución*, 34: 197-232.

Simitis, Spiros (1987). "Reviewing Privacy in an Information Society". *University of Pennsylvania Law Review*, 135(3): 707-746. Disponible en https://scholarship.law.upenn.edu/penn_law_review/vol135/iss3/3, fecha de consulta: 19 de enero de 2026.

Sunstein, Cass R. (1990). *After the Rights Revolution: Reconceiving the Regulatory State*, Cambridge MA: Harvard University Press.

Tapia Gutiérrez, Paloma (2013). *La reparación del daño en forma específica. El puesto que ocupa entre los medios de tutela del perjudicado*. Madrid: Dykinson.

Taruffo, Michele (2005). *La prueba de los hechos*. Madrid: Trotta.

Vergara Blanco, Alejandro (2016). *Principios del Derecho Administrativo*, Legal Publishing, Santiago, pp. 391–397.

Warren, Samuel D., y Brandeis, Louis D. (1890). "The Right to Privacy". *Harvard Law Review*, 4(5), 193-220. https://doi.org/10.2307/1321160

Whitman, James Q. (2004). "The Two Western Cultures of Privacy: Dignity versus Liberty". *Yale Law Journal*, 113(6): 1151-1221. Disponible en https://yalelawjournal.org/article/the-two-western-cultures-of-privacy-dignity-versus-liberty, fecha de consulta: 19 de enero de 2026.

Zuboff, Shoshana (2019). *The Age of Surveillance Capitalism*. New York: PublicAffairs.

Jurisprudencia

20° Juzgado Civil de Santiago, *González López con Clínica Alemana de Santiago,* rol C-20968-2014, 11 de septiembre de 2015.

Boyd v. United States, sentencia de fecha 1 de febrero de 1886.

Carpenter v. United States, sentencia de fecha 22 de junio de 2018.

Corte de Apelaciones de Santiago, *González López con Clínica Alemana de Santiago*, rol 11030-2015, 21 de diciembre de 2015

Corte de Apelaciones de Temuco, *Caminondo con Sistema Nacional de comunicaciones financieras S.A.*, rol N°698-2018, 26 de abril de 2019.

Corte Interamericana de Derechos Humanos, *Baena Ricardo y otros vs. Panamá*, 2 de febrero de 2001.

Corte Interamericana de Derechos Humanos, *Cantos vs. Argentina*, 28 de noviembre de 2002.

Corte Interamericana de Derechos Humanos, *Manuela y otros vs. El Salvador*, 2 de noviembre de 2021.

Corte Suprema, *Berrios con Worldcoin S.P.A. (Grupo Optimistic S.P.A.)*, rol 35.760-2024, 07 de enero de 2025.

Corte Suprema, *Caminondo con Sistema Nacional de comunicaciones financieras S.A.*, rol N°17.667-2019, 03 de julio de 2020.

Corte Suprema, *Conectados S.A. con Empresa Nacional de Comunicaciones S.A. y otros*, rol 11627-2014, 31 de julio de 2014.

Corte Suprema, *Lagos con Ayala*, rol 18.566-2024, 06 de enero de 2025.

Corte Suprema, *Medina con Entel PCS Telecomunicaciones S.A.*, rol N°30.842-2025, 09 de septiembre de 2025,

Dobbs v. Jackson, sentencia de fecha 24 de junio de 2022.

Eisenstadt v. Baird, sentencia de fecha 22 de marzo de 1972.

Griswold v. Connecticut, sentencia de fecha 7 de junio de 1965.

Katz v. United States, sentencia de fecha 18 de diciembre de 1967.

Lawrence v. Texas, sentencia de fecha 26 de junio 2003.

Obergefell v. Hodges, sentencia de fecha 26 de junio de 2015.

Olmstead v. United States, sentencia de fecha 4 de junio de 1928.

Riley v. California, sentencia de fecha 25 de junio de 2014.

Roe v. Wade, sentencia de fecha 22 de enero de 1973.

Tribunal Constitucional español, *La Opinión de Zamora S.A.*, 27/2020, 24 de febrero de 2020.

Tribunal de Justicia de la Unión Europea, sentencia de 19 de octubre de 2016.

Tribunal Supremo español, 188/2022, 15 de febrero de 2022.

Tribunal Supremo español, *Aida con Sociedad de Avalaes y Garantías de Andalucía S.G.R. (SURAVAL)*, 1495/2024, 19 de marzo de 2024.

Normativa

Article 29 Working Party (2018). «Guidelines on security of processing». *WP250* 1:9–11.

Brasil, Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), Seção III ("Responsabilidade e Ressarcimento de Danos"), art. 42.

Children's Online Privacy Protection Act, 21 de octubre de 1998.

Constitución Política de la República de Chile, 22 de septiembre de 2005.

Convención de los Derechos del Niño, 20 de noviembre de 1989.

Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal, 28 de enero de 1981.

Decreto con Fuerza de Ley 1 de 2006, Fija el texto refundido, coordinado y sistematizado de la Ley Nº 18.695, Orgánica Constitucional de Municipalidades, 26 de julio de 2006.

Directrices de la Organización para la Cooperación y el Desarrollo Económico -OCDE- relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales, 23 de septiembre de 1980.

Ley 19.628, sobre Protección de la Vida Privada, 28 de agosto de 1999.

Ley 19.812, modifica la Ley 19.628 sobre protección de la vida privada, 13 de junio de 2002.

Ley 19.899, modifica la Ley 19.848 sobre reprogramación de deudas da los fondos de crédito solidario, 18 de agosto de 2003.

Ley 20.463, modifica Ley 19.628, suspendiendo por el plazo que indica la información comercial de las personas cesantes, 20 de octubre de 2010.

Ley 20.521, modifica la Ley 19.628, sobre protección de datos de carácter personal para garantizar que la información entregada a través de predictores de riesgo sea exacta, actualizada y veraz, 23 de julio de 2011.

Ley 20.575, establece el principio de finalidad en el tratamiento de datos personales, 17 de febrero de 2012.

Ley 20.591, modifica Ley 19.925, sobre expendio y consumo de bebidas alcohólicas, con el objeto de promover las presentaciones de música en vivo, 7 de junio de 2012.

Ley 21.214, modifica la Ley 19.628 sobre protección de la vida privada, con el objeto de prohibir que se informe sobre las deudas contraídas para financiar la educación en cualquiera de sus niveles, 28 de febrero de 2020.

Ley 21.430, sobre Garantías y Protección Integral de los Derechos de la Niñez y Adolescencia, 15 de marzo de 2022.

Ley 21.504, establece prohibición de informar deudas contraídas para financiar servicios y acciones de salud en la Ley 19.628, 10 de noviembre de 2022.

Ley 21.719, que regula la Protección y el Tratamiento de los Datos Personales y Crea la Agencia de Protección de Datos Personales, 13 de diciembre de 2024.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

Memorándum de Montevideo sobre protección de datos personales y la vida privada en las redes sociales en internet, en particular de niños, niñas y adolescentes, 27 y 28 de julio de 2009.

Principios actualizados sobre la privacidad y la protección de datos personales (Informe, 98° período ordinario de sesiones) -OEA / Comité Jurídico Interamericano-, 9 de abril de 2021.

Reglamento 2016/679 del Parlamento y del Consejo Europeo, 27 de abril de 2016.

Reglamento 2022/2065 del Parlamento y del Consejo Europeo, 19 de octubre de 2022.

Resolución 45/95, Asamblea General de la Organización de Naciones Unidas, 14 de diciembre de 1990.

Working Party (WP29), *Opinion 3/2010 on the principle of accountability*, WP 173, 13 July 2010: 9–12.

ACADEMIA
JUDICIAL
CHILE