UNIVERSIDAD DE CHILE

FACULTAD DE DERECHO

DEPARTAMENTO DE DERECHO PÚBLICO

TRATAMIENTO Y PROTECCIÓN DE LOS DATOS PERSONALES EN LA LEY N°19.628: HISTORIA, EVOLUCIÓN, REGULACIÓN, MECANISMOS DE PROTECCIÓN Y DEFICIENCIAS

Memoria de prueba para optar al grado de Licenciado en Ciencias Jurídicas y Sociales

RAÚL CLAUDIO IVÁN GARRIDO VIDAL

PROFESOR GUÍA: DAVID IBACETA MEDINA

SANTIAGO DE CHILE

2024

TABLA DE CONTENIDOS

RESUMEN **1**

INTRODUCCIÓN **2**

CAPÍTULO 1: El derecho a la intimidad **5**

1.1 El origen del derecho a la intimidad 5

1.2 Concepto del derecho a la intimidad 8

1.3 Naturaleza jurídica del derecho a la intimidad 9

1.4 Relación y diferencias entre el derecho a la intimidad con otros derechos 11

1.4.1 Relación y diferencias entre el derecho a la intimidad y el derecho al honor 12

1.4.2 Relación y diferencias entre el derecho a la intimidad y el derecho a la propia imagen 13

1.4.3 Relación y diferencias entre el derecho a la intimidad y el derecho a la información 14

1.4.4 Relación y diferencias entre el derecho a la intimidad con el derecho a la protección de datos personales 15

1.5 El derecho a la intimidad y protección de datos personales ante el desarrollo tecnológico 16

1.6 La autodeterminación informativa 18

1.6.1 La autodeterminación informativa en Chile 19

CAPÍTULO 2: Evolución histórica normativa de la protección de datos personales **20**

2.1 Evolución Histórica Mundial 20

2.1.1 Primera Generación de leyes 21

2.1.2 Segunda generación de leyes 22

2.1.3 Tercera generación de leyes 24

2.2 El reconocimiento Constitucional de la protección de datos personales 30

2.2.1 Reconocimiento Constitucional en Europa 30

2.2.2 Reconocimiento Constitucional en América Latina 32

CAPÍTULO 3: La protección de datos personales 33

3.1 Concepto 33

3.2 Naturaleza jurídica 35

3.3 La protección de datos personales como derecho fundamental 36

3.4 Titularidad de los datos personales 38

3.5 ¿Existe un derecho de propiedad sobre los datos? 38

3.6 Importancia de la protección de los datos personales 39

CAPÍTULO 4: Tratamiento y protección de los datos personales en la Ley N°19.628 42

4.1 Origen de la Ley N°19.628 42

4.2 Estructura de la Ley N°19.628 44

4.3 Modificaciones a la Ley N°19.628 46

4.4 Principios de los datos personales en la Ley N°19.628 50

4.5 Ámbito de aplicación de la Ley N°19.628 55

4.6 Conceptos fundamentales de la Ley N°19.628 56

4.7 Clasificación de los datos personales 59

4.8 Derechos de los titulares de los datos personales 62

4.8.1 Otros derechos de los titulares 66

4.8.2 Límites al ejercicio de los derechos de los titulares 67

4.9 Utilización o tratamiento de los datos personales 68

4.9.1 Utilización de datos personales en obligaciones de carácter económico, financiero, bancario o comercial 69

4.9.2 Tratamiento de datos por los organismos públicos 71

4.10 De la responsabilidad por las infracciones a esta ley 72

4.11 Título Final 73

4.12 Mecanismos de protección 74

4.12.1. El recurso de protección 75

4.12.2 La acción de habeas data 76

CAPÍTULO 5: Deficiencias en la Ley N°19.628 83

5.1 Inexistencia de una autoridad independiente 83

5.1.2 Falta de fiscalización y control 84

5.2 Falta de registros de bancos de datos privados 85

5.3 Críticas a la acción de habeas data 85

5.4 Exclusión de las personas jurídicas 86

5.5 Contradicción en el tratamiento de datos y el principio de finalidad 87

5.6 Crítica a la definición de fuentes accesibles al público 87

5.7 Ineficacia de sanciones y multas 88

5.8 Falta de regulación al flujo internacional de datos 88

5.9 Falta de protección de los datos sensibles 89

5.9.1 Datos sensibles: Vacíos en pandemia 89

5.10 Otras deficiencias en la Ley N°19.628 90

CONCLUSIONES 92

BIBLIOGRAFÍA 98

RESUMEN

La presente memoria trata principalmente sobre el tratamiento y protección de datos personales en la Ley N°19.628 con el fin de comprender su regulación y exponer sus principales deficiencias en la legislación chilena.

Primero, antes de abordar el tema principal, es importante analizar y conceptualizar el derecho a la intimidad, ya que a partir de la evolución de este derecho se origina el derecho de la protección de datos personales, derecho independiente del derecho a la intimidad.

Segundo, una vez entendido el origen del derecho de la protección de datos personales, es esencial el estudio de su historia y evolución mundial, con el fin de exponer la relevancia de este derecho en diversos países a través de diferentes generaciones de leyes, y que incluso en algunos de estos países se constitucionalizó otorgándole el rango de derecho fundamental.

Tercero, la memoria analizará el derecho a la protección de datos personales, su concepto, naturaleza jurídica, titularidad e importancia de su protección. Con lo anterior, la memoria de prueba podrá abordar el tema principal de estudio, al otorgar todos los conceptos básicos, herramientas y análisis pertinentes para lograr comprender la Ley N°19.628.

Cuarto, la memoria expondrá un estudio y análisis de la Ley N°19.628, abordando su origen histórico, modificaciones, conceptualización, regulación legal del tratamiento y protección de datos personales, principios, derechos de los titulares, y su tutela a través de la acción del habeas data con el objetivo de comprender la interpretación de dicha normativa y sus aspectos más relevantes.

Finalmente, al tener una noción global de la Ley N°19.628, permitirá la realización de una exposición y análisis de manera crítica de sus principales deficiencias, visibilizando la necesidad de modificar la Ley N°19.628 con el fin de mejorar la protección de datos personales.

INTRODUCCIÓN

El tratamiento y almacenamiento de datos se remonta a épocas antiguas, pero la informática moderna ha superado las limitaciones físicas y temporales de los archivos. Las bases de datos digitales ocupan menos espacio y permiten el almacenamiento casi ilimitado, agilizando el procesamiento y la distribución de datos. Sin embargo, este avance ha llevado al tratamiento y uso de datos de formas que a menudo escapan del conocimiento de las personas involucradas.

Las leyes de protección de datos, que se originaron en Europa en los años 70, inicialmente se basaron en el respeto por la privacidad y la intimidad. Con el tiempo, estas legislaciones de protección de datos personales evolucionaron hacia el reconocimiento constitucional como nuevo derecho fundamental, debido a las cambiantes necesidades técnicas y actuales.

La investigación acerca de la protección de datos personales se origina por la creciente conectividad digital en nuestro mundo. En particular, en el contexto de circunstancias sanitarias recientes en el mundo en relación con el COVID-19, esta interconexión ha asumido un papel central en la sociedad. La era de la información se manifiesta de manera más notable que nunca, en donde la red y las plataformas moldean gran parte de nuestra vida diaria.

En la actualidad, el estudio de los datos personales va más allá de asegurar la intimidad, se trata de preservar nuestra identidad y privacidad en esta sociedad digital en constante expansión, impulsada por avances tecnológicos, ya que su tratamiento incorrecto puede resultar en la vulneración de los datos personales de sus titulares. En respuesta a esta realidad, emerge el derecho de la protección de datos personales como una consecuencia de las nuevas Tecnologías de la Información y Comunicación (TICs).

Las ventajas del tratamiento de datos, tanto por el Estado como por particulares, chocan con la necesidad de proteger los datos personales de las personas, una necesidad constante. Una sociedad que puede gestionar vasta información ya sea por entidades públicas o privadas, y realizar tratamientos instantáneos que pueden cruzar fronteras en momentos, representa un riesgo potencial para sus ciudadanos.

En particular, las personas son dueñas de su información personal y un uso inapropiado por terceros podría infringir derechos fundamentales como la dignidad, igualdad, libertad de expresión, honra, intimidad y vida privada. En consecuencia, es crucial mejorar la regulación, siguiendo estándares internacionales. Estos derechos ahora enfrentan nuevos desafíos, haciendo crucial la creación de legislaciones para proteger los datos personales.

En Chile, la regulación se encuentra en la Ley N°19.628, "Sobre protección de la vida privada", esta ley específicamente aborda la protección de datos personales. Asimismo, cabe mencionar, que el artículo 19 N°4 de la Constitución de Chile le otorga rango constitucional a la protección de datos personales de sus titulares, siendo este un derecho fundamental. La razón detrás de abordar este tema es la problemática que enfrenta Chile. A pesar de contar con una ley para la protección de datos personales, esta se encuentra desactualizada. Aunque, en el Congreso hay múltiples proyectos de ley que buscan actualizar y mejorar la regulación actual sobre la protección de datos personales, con el objetivo de modernizar la normativa y superar sus actuales deficiencias.

Con la presente memoria busco exponer la relevancia que posee el derecho de la protección de datos personales para las personas en la sociedad, sobre todo en la sociedad chilena, ya que este mismo se desenvuelve cada vez más en un ambiente más tecnológico que evoluciona rápidamente, insertándose en nuestras vidas en diferentes aspectos, por ello busco contribuir a un mejor desarrollo de este tema en la doctrina nacional.

El objetivo de la presente memoria principalmente es explicar y analizar el tratamiento y protección de datos personales en la Ley N°19.628 con el propósito de comprender su regulación y exponer sus principales deficiencias en la legislación chilena, visibilizando la necesidad de modificar la Ley N°19.628 con el fin de mejorar la protección de datos personales.

Por lo tanto, la memoria se realizará con la siguiente estructura metodológica:

En el Capítulo 1, describiré la evolución del derecho a la intimidad que dio origen al derecho a la protección de datos personales, partiré analizando el origen, historia y evolución del derecho a la intimidad, para luego desarrollar el concepto y naturaleza jurídica del derecho a la intimidad. Posteriormente, se distinguirá y se expondrá la relación del derecho a la intimidad con otros derechos, todos estos independientes, aunque comparten similitudes con el derecho a la intimidad, tales como, el derecho al honor, el derecho a la propia imagen, el derecho a la información, y el derecho a la protección de datos personales. Luego, se abordará la relación que existe entre el derecho a la intimidad y el derecho a la protección de datos personales ante el desarrollo tecnológico. Finalmente, se explicará en este capítulo el derecho a la autodeterminación informativa en general, para concluir con la situación del derecho a la autodeterminación informativa en Chile.

En el Capítulo 2, explicaré la evolución histórica normativa del derecho a la protección de datos personales con el fin de otorgar mayor contexto de su importancia a través del tiempo. Se analizará su evolución histórica mundial, las diferentes generaciones de leyes según el contexto histórico, y el

reconocimiento de la protección de datos personales en el ámbito constitucional europeo y latinoamericano.

En el Capítulo 3, se analizará la protección de datos personales, abordando su concepto, naturaleza jurídica, la protección de datos como derecho fundamental, la titularidad de los datos personales. También, se analizará si es que existe derecho de propiedad sobre los datos, y finalmente se expondrá la importancia de la protección de los datos personales.

En el Capítulo 4, se analizará profundamente la regulación establecida en la Ley N°19.628, explicando su origen histórico, estructura, modificaciones realizadas desde su origen hasta la actualidad, principios de los datos personales, su ámbito de aplicación, conceptos fundamentales, clasificación de los datos personales, derechos de los titulares, utilización y tratamiento de los datos personales, responsabilidad por las infracciones a la ley, mecanismos de protección de los datos personales, los que incluye el recurso de protección y la acción de habeas data, entre otras materias que aborda la ley.

Finalmente, en el Capítulo 5, estará dedicado especialmente a exponer y a analizar las principales deficiencias de la Ley N°19.628, visibilizando la necesidad de modificar la Ley N°19.628 con el fin de mejorar la protección de datos personales.

CAPÍTULO 1: El derecho a la intimidad

1.1 El origen del derecho a la intimidad

Existen diversas épocas en la historia de la humanidad en que se ha desarrollado el concepto de la "intimidad", la cual es esencialmente humana y ha estado desde el origen de la historia del ser humano. Sin embargo, la noción de intimidad en las distintas épocas ha tenido diferentes niveles de importancia o conceptualización, en las cuales se ha desarrollado, incluso en la antigüedad griega y romana, se describen los beneficios del aislamiento y la meditación, pero dicha conceptualización aún es muy preliminar, y dicha noción no es la misma que se entiende hoy por intimidad.

En la antigüedad, la noción de intimidad no tenía la misma relevancia, y no es hasta finales de la edad media sostener su aparición de forma similar a como se conoce hoy, en la cual se sostiene que la intimidad es propia de las personas y que se trata de la conciencia que cada uno de nosotros tiene como sujeto único e irrepetible. Se hace una distinción entre la interioridad y la intimidad. La interioridad la tienen todos los seres materiales. En cambio, la intimidad sólo la tienen los seres racionales, definiéndola como el núcleo más oculto de cada persona, donde se proyectan los pensamientos y decisiones más propias del ser humano. Esta es una de las primeras definiciones del concepto intimidad, aproximación que procede de la filosofía, y que con posterioridad sirve como base a la elaboración de conceptos del ámbito jurídico.

La noción de intimidad se relaciona con la posibilidad de aislamiento físico del individuo, definiendo inicialmente el derecho a la intimidad como "el derecho a estar solo o a no ser molestado"[1].

Es en la segunda mitad del siglo XIX donde se vislumbra un cambio radical en torno a la elaboración jurídica y doctrinal del derecho a la intimidad. En 1890 los juristas norteamericanos Warren y Brandeis en su monografía "The Right to Privacy" presentaron la necesidad de reconocer el derecho a la intimidad, fundamentado en base en el principio de la inviolabilidad de la persona, pretendiendo establecer límites jurídicos con el objetivo de impedir continuas intromisiones de la prensa en la vida privada de las personas. Ambos juristas estudiaron las normas y principios del Common Law, concluyendo que "el derecho a la intimidad se caracteriza por el rechazo a toda intromisión no consentida"[2]. Se constituye así el derecho a la intimidad como un derecho de no interferencia, ligado con el principio de la inviolabilidad de la persona. El derecho de la intimidad se extiende a la apariencia física

[1] GARRIGA, A. (2016). Nuevos retos para la protección de datos personales: en la era del Big Data y de la computación ubicua. Nuevos retos para la protección de datos personales, Madrid, Dykinson. p. 68.
[2] LUCAS MURILLO DE LA CUEVA, P (1990). El derecho a la autodeterminación informativa. Madrid, Tecnos. p. 60.

personal, relaciones personales, hechos, dichos, pensamientos, emociones y sensaciones, que se expresen ya sea por escrito, conversación, actos o gestos.

Con anterioridad John Stuart Mill elaboró una teoría sobre el derecho a protegerse de intromisiones ajenas, su idea era la de la independencia absoluta con el fin de preservar al individuo de la sociedad de masas.

En 1902 la Corte de Apelaciones de Nueva York, "en el caso Roberson, admite sin reserva la teoría de Warren y de Brandeis, y a partir de ese momento se multiplican las resoluciones judiciales al respecto"[3].

En 1960, Estados Unidos, William Prosser publica un ensayo en base a la teoría de Warren y Brandeis que identifica posibles violaciones del derecho a la intimidad.

En 1961, Reino Unido, se crean diferentes proyectos de ley para la creación de un derecho autónomo a la intimidad. El primer proyecto presentado es el de Lord Mancroft el 14 de febrero de 1961, posteriormente en 1967 el Proyecto de Lyon, con el objetivo de "proteger de toda interferencia irracional y seria que viole la separación entre el público y la persona misma, su familia o su propiedad"[4], ambos proyectos buscan garantizar la intimidad frente a intromisiones de medios de comunicación de masas. En 1967 se presenta el proyecto Baker, que trata el problema de la informática en relación con la protección de la información personal. En 1969, Brian Walden presenta un nuevo proyecto, en relación con el impacto computacional sobre la vida privada, presentándose el problema de los bancos de datos personales. Posteriormente se crean otros proyectos, como el de Kenneth Baker de 1969, Leslie Huckfield de 1971 y el Right of Privacy Bill del National Council for Civil Liberties de 1971, en estos proyectos se propone controlar los bancos de datos personales contenidos en los ordenadores computacionales.

Por otra parte, en Europa, los orígenes del derecho a la intimidad se encuentran en la doctrina de los derechos de la personalidad, que se origina del seno del derecho civil. Los derechos de la personalidad son derechos esenciales e inviolables y que están en continuo movimiento, ya que se fundan de la propia esencia humana, se deben de adaptar a las nuevas circunstancias y necesidades sociales de la época histórica. El derecho a la intimidad se reconoce en las constituciones posteriormente, después de que se

[3] GARRIGA, A. (2016). Nuevos retos para la protección de datos personales: en la era del Big Data y de la computación ubicua. Nuevos retos para la protección de datos personales, Madrid, Dykinson. p. 69.
[4] LOSANO, M. (1989). "Los orígenes de la Data Protection Act inglesa de 1984", en LOSANO, Mario, PÉREZ LUÑO, Antonio E., y GUERRERO MATEUS, Mª Fernanda.: Libertad informática y leyes de protección de datos personales, Madrid, Centro de Estudios Constitucionales. p. 19.

hayan reconocido otros derechos relacionados, como el secreto de las comunicaciones y la inviolabilidad del domicilio.

El reconocimiento del derecho a la intimidad se produce de forma difusa, pero se distinguen tres niveles diferentes: 1) Constitución que reconozca de forma explícita y plena el derecho a la intimidad, haciendo referencias genéricas. 2) Que establezcan simples manifestaciones del derecho a la intimidad. 3) Que no se establezcan referencias ni manifestaciones del derecho a la intimidad.

En la esfera internacional, el derecho a la intimidad es establecido en el artículo 12 de la Declaración Universal de los Derechos Humanos de 10 de diciembre de 1948, estableciendo que:

> "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".[5]

Asimismo, y casi en términos similares se estableció en el artículo 17 del Pacto Internacional de Derechos Económicos, Sociales, Civiles y Políticos de 16 de diciembre de 1966.

En la esfera europea, el artículo 8 del Convenio de Roma de 4 de noviembre de 1950 para la Protección de los Derechos Humanos y de las Libertades Fundamentales contiene el derecho al respeto a la vida privada y familiar. Por otra parte, en América se establece el derecho a la intimidad en el artículo 11 de la Convención Americana sobre Derechos Humanos que garantiza la protección de la honra y de la dignidad.

El origen histórico de la idea de identidad se encuentra en el momento de la construcción del Estado liberal, apareciendo la burguesía y el individualismo, pero su mayor desarrollo se produce en el siglo XX. En su evolución, lo íntimo y lo privado se desarrolla a costa de lo público. La vida íntima y privada crece debido a las ideas de libertad mientras se limita el poder público, producto de lo anterior, se origina el derecho a la intimidad. Para los liberales, la libertad está íntimamente relacionada con la existencia de este dominio privado. Además, gran influencia en el concepto de intimidad burguesa tiene la Reforma protestante al conseguir,

> "transformar radicalmente los hábitos seculares y, especialmente, los que regían dentro de las paredes de las casas haciendo, a partir de ahora, de la reclusión, de los diarios personales

[5] ONU: ASAMBLEA GENERAL. (1948). Declaración Universal de los Derechos Humanos. (217 [III] A). Paris. Recuperado el 15 de abril de 2023, de http://www.un.org/en/universal-declaration-human-rights/

y de la lectura familiar de la Biblia acciones cotidianas que serán básicas en la formación de la vida privada".[6]

Otros ámbitos que originaron la idea de intimidad que contribuyeron en el desarrollo del individualismo moderno, son la alfabetización, la búsqueda de la soledad y del retiro.

El derecho de la intimidad como derecho a la soledad y a la reserva coincide cronológicamente con el fenómeno de la revolución y la afirmación de los derechos del hombre, en que el derecho a la intimidad se sitúa al margen de la intromisión estatal.

1.2 Concepto del derecho a la intimidad

El derecho a la intimidad en el Diccionario de la Real Academia Española se define como: "Derecho a disfrutar de un ámbito propio y reservado para desarrollar una vida personal y familiar plena y libre, excluido tanto del conocimiento como de las intromisiones de terceros"[7]. Esta es una definición más coloquial del concepto, pero es necesario precisarlo al ámbito jurídico, cuyo concepto es más complejo que dicha definición.

Definir el derecho a la intimidad es complejo, pero la doctrina establece una relación directa con la esfera más cercana e íntima de la persona, por ende, la persona tiene derecho a decidir por sí misma en qué medida desea compartir su vida personal, sentimientos, pensamientos. Es innegable que el ser humano es por naturaleza un ser social, pero es esa misma naturaleza el fundamento del derecho a la intimidad, ya que cada persona precisa de mantener y conservar una vida personal, ajena a las relaciones externas con otras personas, por su necesidad de desarrollo a su libertad interior, garantizando su dignidad humana. El bien jurídico protegido por el derecho a la intimidad es el modo de ser interno de la persona, excluido el conocimiento de terceros, porque su descubrimiento le ocasionaría una perturbación en su dignidad como persona humana, lo cual vulneraría su desarrollo personal e interior. Cabe añadir, que el derecho a la intimidad representa el derecho de cada persona a decidir sobre la información y su vida privada, revelando solo aquello que se quiera compartir con terceros, esto asegura una calidad de vida mínima de vida en las relaciones con terceros. Fariñas señala lo siguiente:

> "diferencia el autor un derecho objetivo, como reconocimiento que el ordenamiento jurídico dispensa al derecho a la intimidad, y un derecho subjetivo a la intimidad, entendido como facultad del hombre, esgrimible erga omnes, consistente en poder graduar la relación con

[6] MARTÍNEZ DE PISÓN CAVERO, J. (1993). El derecho a la intimidad en la jurisprudencia constitucional. Madrid, Citas. p. 40.
[7] REAL ACADEMIA ESPAÑOLA. Diccionario de la Lengua Española. Recuperado el 3 de mayo de 2023, de https://dpej.rae.es/lema/derecho-a-la-intimidad.

el exterior, y que comporta la posibilidad de solicitar el pertinente amparo del ordenamiento jurídico cuando dicha facultad sea transgredida."[8]

El derecho a la intimidad constituye una manifestación de la dignidad humana, la cual se refiere al derecho de las personas a mantener en reserva su vida privada y familiar, protegiendo su esfera personal de la intromisión arbitraria o ilegítima de terceros o del Estado, asegurando el respeto de la dignidad humana.

En la legislación chilena, en el marco de la protección de datos personales de la Ley N°19.628 "Sobre la protección de la vida privada", norma que subyace del artículo 19N°4 de la Constitución de Chile, trata como sinónimos, tanto el legislador, como la doctrina, los conceptos de intimidad y vida privada.

Según se describe en la doctrina nacional, el derecho a la intimidad está establecido en el artículo 19 N°4 de la Constitución de Chile, bajo la denominación de "vida privada", junto con otros dos conceptos, la vida pública, y la honra de la persona y de su familia. Para García, la intimidad es "el derecho a no ser conocidos, en ciertos aspectos por los demás. Es un derecho al secreto, a que los demás no sepan lo que somos o lo que hacemos"[9].

En resumen, se entiende el derecho a la intimidad, como la capacidad de las personas de mantener un ámbito interno en reserva, teniendo el derecho a decidir y controlar la información y vida íntima de la forma que cada persona desee, pudiendo determinar libremente a quienes comparte su intimidad.

1.3 Naturaleza jurídica del derecho a la intimidad

En primera instancia, se identificaba el derecho a la intimidad en relación con el derecho de propiedad, esta concepción fue abandonada por la doctrina, pues limitaba su ámbito de protección a los ataques materiales a los espacios propios en donde se ejerce el derecho. La protección del derecho a la intimidad se expandió en cosas inmateriales o espirituales como la soledad y el retiro, por ende, ya no podía fundarse en el derecho a la propiedad. Se determina entonces, que emana el derecho a la intimidad de la dignidad de la persona humana, de su inviolabilidad, situación jurídica que es reconocida en diversos tratados internacionales de derechos humanos y en distintas Constituciones, entre ellas la Constitución Chilena de 1980. Constitucionalmente el concepto de intimidad se define como el ámbito

[8] HERRÁN, A. (2003). El derecho a la protección de datos personales en la sociedad de la información. España, Ed. Universidad de Deusto. p. 12.
[9] VÁSQUEZ, E. E. (2004). El Hacking No Es (Ni Puede Ser) Delito. Revista Chilena de Derecho Informático, (4). p. 162.

más próximo de la persona en relación con la dignidad de la persona humana. El derecho a la intimidad es un derecho humano de carácter individual, no de carácter social.

El derecho a la intimidad puede ser estudiado desde tres áreas distintas. Desde el área del derecho civil, es un derecho de la personalidad. Desde el área constitucional es un derecho fundamental. Por último, desde el área de los derechos humanos en los tratados internacionales como un derecho humano, ya que emana de la dignidad de la persona.

Desde el punto de vista constitucional es un derecho fundamental, además desde el punto de vista de los derechos humanos en los tratados internacionales es un derecho humano. Los derechos fundamentales son derechos humanos reconocidos y garantizados en las constituciones, siendo garante el Estado, mientras que los derechos humanos están reconocidos y garantizados en normas de carácter internacional como los tratados internacionales, siendo garante la comunidad internacional. Al tratarse el derecho a la intimidad como un derecho fundamental, el titular de este derecho subjetivo de derecho público tiene la facultad de exigir su respeto al Estado y los particulares, y que se garanticen a través de un órgano jurisdiccional en caso de que dicho derecho sea vulnerado o impedido su ejercicio, solicitando la protección del derecho y la reparación del daño.

Los derechos fundamentales, entre ellos el derecho a la intimidad, se caracterizan por tener una doble perspectiva. En primer lugar, como derecho subjetivo como de defensa es un concepto jurídico que se refiere al derecho que tiene toda persona de hacer valer sus derechos ante los tribunales y de recibir protección jurídica efectiva ante una vulneración o amenaza. En segundo lugar, como derecho de libertad o garantía positiva, se refiere a la obligación del Estado de proteger y asegurar el ejercicio efectivo de los derechos fundamentales de las personas. Esta doble perspectiva está reconocida en el artículo 5, inciso segundo y artículo 6 de la Constitución de Chile. En este sentido, la doble perspectiva de los derechos fundamentales implica que,

> “se ha superado la tradicional concepción del derecho a la intimidad como derecho a ser dejado en paz, para acoger en su ámbito una esfera de protección positiva, que se manifiesta en el reconocimiento de determinadas facultades para exigir y facilitar un ámbito de libertad y el pleno ejercicio de los derechos de las personas; en definitiva, se aspira a garantizar el control de la información que nos concierne y que otros conocen de nosotros, no se trata de reaccionar cuando nuestra intimidad se ha visto vulnerada, sino de exigir positivamente del Estado deberes

de tutela del derecho, y en todo caso, de garantizar facultades para la tutela y defensa de las libertades de la persona."[10]

Por último, desde el punto de vista del derecho civil, es un derecho de la personalidad, refiriéndose a relaciones intersubjetivas del ser humano con sus semejantes en situación de igualdad. El derecho a la intimidad es un derecho de la personalidad porque,

> "constituye un bien instrumental para garantizar la libertad del individuo en el desarrollo de su propia vida. Luego, la libertad individual se erige en fundamento necesario de la dignidad humana, y el derecho a la intimidad se configura como elemento esencial para el desarrollo de la personalidad."[11]

1.4 Relación y diferencias entre el derecho a la intimidad con otros derechos

Inicialmente el derecho a la intimidad se entendió que comprendía otros derechos de la personalidad como el derecho al honor y el derecho a la propia imagen, otorgándole una concepción amplia. Pero, posteriormente, se reconoció la autonomía de estos tres derechos, independientes entre sí, pero que están estrechamente relacionados, debido a que estos tres derechos son derechos de la personalidad.

A menudo se confunden como si se tratara de un único concepto los derechos al honor, a la intimidad y a la propia imagen. En muchas ocasiones tanto la prensa, ya sea escrita o audiovisual, como en muchas demandas se trata de forma indiferenciada estos derechos, extendiéndose incluso a la jurisprudencia. Por tanto, los derechos al honor, a la intimidad y a la propia imagen, la confusión se debe a que,

> "tienen en común el ir muy ceñidos a la propia persona, proteger su entorno espiritual más próximo (…); ser, como otros derechos de la personalidad, pero más aún si cabe, «personalísimos» de su titular; y, sin perjuicio de ciertas dimensiones o manifestaciones de los mismos (…), sólo existen en vida del interesado."[12]

Sin embargo, existen elementos diferenciadores entre estos derechos que analizaremos a continuación.

---

[10] HERRÁN, A. (2003). El derecho a la protección de datos personales en la sociedad de la información. España, Ed. Universidad de Deusto. p.11.
[11] HERRÁN, A. (2003). El derecho a la protección de datos personales en la sociedad de la información. España, Ed. Universidad de Deusto. p. 10.
[12] LACRUZ, J. (1990). Elementos de derecho civil, I; Parte general del Derecho Civil, Volumen segundo, Personas, Barcelona, Ed. José María Bosch. p. 71-72.

1.4.1 Relación y diferencias entre el derecho a la intimidad y el derecho al honor

El derecho al honor es un derecho fundamental distinto al derecho a la intimidad, ya que el derecho al honor es un derecho independiente al de la intimidad, porque el derecho al honor es inherente a toda persona y protege su integridad moral y la dignidad humana, el derecho que tiene todo ser humano a ser tratado conforme con su dignidad y que se manifiesta de acuerdo con la estimación que él siente sobre sí mismo y que espera de los demás.

En el derecho al honor se distinguen dos aspectos: El primer aspecto es el subjetivo o interno que "es definido como el aprecio o estimación que el ser humano tiene por sí mismo y cuya violación conlleva un claro menosprecio hacia la persona"[13],en síntesis, se refiere a la propia estima que el individuo se tiene. El segundo aspecto es el objetivo o externo, "que se concreta en el interés de toda persona por el prestigio, reputación o buen nombre que goce ante los demás"[14], esto en referencia a la reputación o fama de la persona.

Del análisis anterior con respecto a la definición del derecho al honor y sus dos aspectos, el subjetivo y el objetivo, se diferencia el derecho al honor con el derecho a la intimidad, debido a que el derecho a la intimidad se refiere a mantener en secreto ese círculo íntimo, personal y familiar que toda persona posee, es algo íntimo de la persona que guarda para sí, y que su titular desea mantener fuera del conocimiento de las demás personas, lo cual es muy diferente a lo que expone el derecho al honor, que se manifiesta en el respeto a nuestra reputación o fama, y en la estima que el individuo tiene sobre sí mismo.

Con el fin de establecer una mayor distinción entre ambos derechos, analizaremos a continuación dos elementos diferenciadores: a) el bien jurídico protegido y b) el modo en que se produce la agresión al derecho al honor y al derecho a la intimidad.

El bien jurídico protegido: El derecho al honor protege el bien jurídico de la honra, la propia estima y la estima en que nos tienen los otros. En cambio, el derecho a la intimidad el bien jurídico protegido es la decisión de mantener en secreto, en su fuero interno una parte de su vida.

El modo en que se produce la agresión al derecho al honor y al derecho a la intimidad: Primero, en cuanto al derecho al honor, es esencial en la agresión al honor que el ofensor actúe con la intención de injuriar, ya que es necesario un elemento subjetivo, el cual es el ánimo de injuriar, para que la agresión

[13] MARTÍNEZ DE PISÓN CAVERO, J. (1993). El derecho a la intimidad en la jurisprudencia constitucional. Madrid, Citas. p. 101.
[14] MARTÍNEZ DE PISÓN CAVERO, J. (1993). El derecho a la intimidad en la jurisprudencia constitucional. Madrid, Citas. p. 102.

se produzca, sin que importe que el hecho pertenezca a la vida privada. En cambio, en el derecho a la intimidad, no es necesaria ningún tipo de intención, ni de injuriar, ni de insultar, ni de despreciar, para vulnerar la intimidad de la persona, ya que "el que descubre una parcela vital mantenida en secreto o, simplemente, reservada, invade la intimidad del afectado, con total independencia de cuál sea la intención que le haya movido"[15] , esto quiere decir que basta para vulnerar el derecho a la intimidad con entrometerse ilegítimamente en el ámbito interno de una persona que quiere mantener en secreto, fuera del conocimiento de las demás personas.

Debido a lo analizado anteriormente, se concluye que el derecho a la intimidad y el derecho al honor son dos derechos distintos. Ambos, son derechos fundamentales que se consagran constitucionalmente usualmente en una misma disposición constitucional, pero ambos protegen distintos bienes jurídicos. Por otra parte, cabe distinguir, que el derecho a la intimidad se vulnera cuando se afecta aquella parte de la personalidad que se ha decidido mantener en secreto frente a los demás. Mientras el derecho al honor se vulnera a la persona cuando a esta se la desprecia y se ataca su reputación.

Puede suceder que de un mismo hecho de agresión no solo suponga un atentado al honor o a la intimidad, sino que puede ocurrir que de un mismo hecho se vulnere no solo a un derecho, sino que, a ambos derechos, lo cual debe ser analizado en el caso concreto.

Para concluir, el honor y la intimidad son presupuestos de la participación del individuo en la sociedad, pero apuntan a momentos distintos.

> "El honor está en contacto directo con la participación del individuo en la comunidad; en la intimidad, por el contrario, lo que se pretende es, en último término, garantizar un ámbito de no intervención activa en la vida social, bien a través de asegurar la falta de información, bien mediante el control sobre dicha información."[16]

1.4.2 Relación y diferencias entre el derecho a la intimidad y el derecho a la propia imagen

El derecho a la propia imagen es un derecho fundamental autónomo basado en la dignidad humana, que resguarda la dimensión moral de las personas. Este derecho permite al individuo controlar la difusión pública de su imagen generada a partir de sus características físicas personales. Esencialmente, este derecho fundamental impide que terceros no autorizados obtengan, reproduzcan o

[15] BUSTOS, J. (1992). Los límites de los derechos de libre expresión e información según la jurisprudencia, en García San Miguel, Luis: Estudios sobre derecho a la intimidad. Madrid, Tecnos. p. 135.
[16] BERDUGO GÓMEZ DE LA TORRE, I. (1987). Honor y libertad de expresión. Madrid, Tecnos. p. 62.

publiquen la propia imagen, independientemente de la finalidad, ya sea informativa, comercial, científica, cultural, u otra, que persigan al captar o difundir dicha imagen.

El derecho a la propia imagen se relaciona estrechamente con el derecho al honor y con el derecho a la intimidad, ya que estos tres son derechos de la personalidad que derivan de la dignidad de la persona. Cabe mencionar, que es muy recurrente que por la captación y divulgación de la imagen de una persona pueda vulnerarse tanto su honor como su intimidad, dependiendo del caso concreto. El derecho a la propia imagen buscar proteger un ámbito propio y reservado ante la acción y conocimiento de los demás, pero no íntimo como el derecho a la intimidad.

El derecho a la propia imagen es el derecho que busca controlar la captación, reproducción, divulgación de los rasgos físicos que identifican a una persona para proteger su esfera moral y su libre desarrollo, garantizando un ámbito privado libre de intromisiones extrañas. Se puede distinguir dentro del derecho a la propia imagen un aspecto positivo y otro negativo. En el aspecto positivo es "el derecho a obtener, reproducir y publicar la propia imagen"[17]. Por otra parte, el aspecto negativo se basa en "excluir la mera obtención o la reproducción y publicación de la propia imagen por un tercero que carece del consentimiento del titular para ello"[18].

La relación entre el derecho a la propia imagen y el derecho a la intimidad es debido al origen del derecho a la propia imagen como un subtipo o representación del derecho a la intimidad, al que se le consideró por mucho tiempo como el único derecho de la personalidad. Sin embargo, ambos derechos son diferentes, ya que el derecho a la propia imagen consiste en que es el derecho que busca controlar la captación, reproducción, divulgación de los rasgos físicos que identifican a una persona para proteger su esfera moral y su libre desarrollo, garantizando un ámbito privado libre de intromisiones extrañas como se mencionó anteriormente. Mientras, el derecho a la intimidad se refiere a mantener en secreto ese círculo íntimo, personal y familiar que toda persona posee, es algo íntimo de la persona que guarda para sí, y que su titular desea mantener fuera del conocimiento de las demás personas.

1.4.3 Relación y diferencias entre el derecho a la intimidad y el derecho a la información

El derecho a la intimidad y el derecho a la información son derechos fundamentales que están protegidos en la mayoría de los sistemas jurídicos modernos, incluyendo el ordenamiento jurídico

[17] MUÑOZ, X.O.C. (1991). Libertad de expresión y sus límites: honor, intimidad e imagen. Madrid, Editoriales de Derecho Reunidas. p. 117.
[18] MUÑOZ, X.O.C. (1991). Libertad de expresión y sus límites: honor, intimidad e imagen. Madrid, Editoriales de Derecho Reunidas. p. 117.

chileno. Ambos derechos son importantes para proteger los derechos humanos y la dignidad de la persona humana, pero en ocasiones entran en conflicto entre sí.

Por un lado, el derecho a la intimidad se refiere al derecho de las personas a mantener su vida privada y familiar protegida de la intromisión arbitraria o ilegítima de terceros o del Estado. Por otro lado, el derecho a la información se refiere al derecho de las personas a buscar, recibir y difundir información y a estar informados sobre asuntos de interés público, dicho derecho se establece en el artículo 19 N°12 de la Constitución de Chile.

Pero, en algunos casos estos derechos entran en conflicto, como cuando una publicación con información privada viola la intimidad de una persona. En tales casos, se debe equilibrar estos derechos en conflicto.

El Tribunal Constitucional Chileno ha señalado que el derecho a la intimidad, pese a que es un derecho fundamental para la autonomía individual y para la dignidad personal, no es un derecho absoluto, por ende, puede "ceder ante la prevalencia de otros derechos, como el derecho a la información cuando se refiere a hechos con relevancia pública, en el sentido de noticiables, y que dicha información sea veraz"[19]. Sin embargo, cualquier restricción al derecho a la intimidad debe ser necesario y proporcionado, y no puede ser más amplio de lo necesario para proteger el interés público en cuestión.

1.4.4 Relación y diferencias entre el derecho a la intimidad con el derecho a la protección de datos personales

El derecho a la protección de datos personales se encuentra profundamente vinculado con el derecho a la intimidad, ya que la protección de los datos personales tiene su origen con la necesidad de proteger la intimidad y la vida privada de las personas. El derecho a la protección de datos personales ha ido evolucionando debido a los grandes avances tecnológicos contemporáneos de la era digital que impactan la vida cotidiana de las personas, en relación con las nuevas tecnologías de la información y comunicaciones, por ello existe la necesidad de proteger los datos personales, confiriéndole a sus titulares la facultad de poder controlar dicha información.

El desarrollo de la tecnología ha impactado considerablemente a las instituciones jurídicas, por ende, existe la necesidad de proteger el derecho a la intimidad, entre otros derechos de la personalidad como el honor, la propia imagen, con el fin de resguardar la dignidad de las personas, por estos mismos motivos, existe la necesidad de proteger los datos personales. Con el surgimiento de la tecnología, el

[19] MEZA-LOPEHANDÍA, M. (2016). Libertad de expresión y protección de la intimidad: Chile, España y México. Santiago, Biblioteca del Congreso Nacional de Chile. p. 3.

derecho a la intimidad se ha debido reformular, pasando desde una visión negativa inicialmente del derecho a estar sólo, es decir, la no interferencia de terceros, hacia una visión positiva, confiriéndole al titular de los datos una serie de facultades para poder controlar la información de sus datos que son almacenados, procesados o suministrados por terceras personas, y por este mismo motivo, el derecho a la intimidad fue evolucionando a través del tiempo, permitiendo el desarrollo y origen del derecho de la protección de datos personales. Entonces, el antecedente inicial para el desarrollo de la protección de datos personales es el derecho a la intimidad, por este mismo motivo, el derecho de la protección de datos personales es independiente al derecho a la intimidad, ya que:

> "Pese a ser la intimidad o la vida privada el fundamento último de protección, se hace necesario en el ámbito del reconocimiento y garantía de los derechos y libertades fundamentales, la especialización. Ésta es la circunstancia dada en lo relativo a la protección de datos, que, sin abandonar la fundamentación originaria, ha evolucionado de forma muy significativa, incluso podríamos decir que adquiere autonomía, se independiza del derecho originario, como ha ocurrido en la historia de los derechos humanos en muchas ocasiones."[20]

Por lo tanto, el derecho a la protección de datos personales contiene características diferentes al derecho a la intimidad, surgiendo en el mundo la creación de distintas leyes sobre la protección de datos personales.

1.5 El derecho a la intimidad y protección de datos personales ante el desarrollo tecnológico

El desarrollo tecnológico representa un riesgo para el tratamiento y el almacenamiento de la información y datos de las personas. Por ello los datos personales, en su tratamiento, almacenamiento, uso, control, debe ser reconocido no solo como una garantía, sino como un derecho fundamental protegido a nivel constitucional.

Las redes sociales e internet han supuesto una revolución en la sociedad, y se consideran como elementos esenciales para nuestras actividades cotidianas debido a su uso práctico, por ejemplo, trabajar, comprar, relacionarnos por redes sociales con nuestros amigos, etc. Del mismo modo que ha supuesto un cambio radical en nuestras vidas, asimismo se configura el desarrollo tecnológico en el ámbito de las redes sociales e internet como el medio idóneo para la lesión de nuestros derechos como los derechos al honor, a la intimidad, a la propia imagen, a la información y la protección de datos personales.

[20] REBOLLO, L. (2008). Vida privada y protección de datos en la Unión Europea. España, Dykinson. p. 94.

En cuanto a la intimidad, la problemática recurrente en internet y las redes sociales se centran en el tema de la protección de datos. La protección de datos personales en el marco de internet y las redes sociales es de gran importancia, ya que desde el momento en que ingresamos a internet, dejamos huellas de nuestra actividad, sobre todo por la función que realizan las "cookies". Las cookies permiten a los sitios web recordar información de nuestras visitas, facilitando futuras visitas y mejorando la utilidad de los sitios. Hay que tener en consideración que acceder a internet o crearse una cuenta en una red social es gratuito, pero tal como señala la doctrina tiene un valor extraordinario,

> "porque gracias a ella la información, el mensaje o la publicidad son personalizadas. El proveedor, o el anunciante, ya no se dirigen a categorías de internautas sino a sujetos concretos. Y lo que es más importante, tienen la capacidad de establecer o identificar círculos de confianza y gracias a ellos la viralidad de los mensajes multiplica la eficiencia y la eficacia de los tratamientos"[21].

Por otra parte, otros autores señalan que las redes sociales se basan en la confianza y que la confianza se obtiene con el conocimiento del otro, y por ello, "esto provoca que se considere que habitualmente que cuanta más confianza hay, más datos personales identificables (PII, en inglés) del otro se desea tener y, por tanto, más riesgo para la privacidad"[22]. Las redes sociales como Instagram, Facebook, Tiktok, entre otras que se basan en la creación de perfiles, provoca que sus usuarios publiquen una considerable cantidad de datos personales, pese a que los mismos usuarios puedan determinar el nivel de privacidad o del círculo de personas que puedan acceder a sus contenidos, no llegan a ser conscientes de los efectos que pueda producir compartir tanta información. La doctrina advierte que, al publicar contenido en plataformas accesibles para todos los usuarios, los perfiles personales quedan expuestos y existe el peligro de perder el control sobre la información en internet. Esto puede generar un riesgo mayor que en interacciones presenciales. Es importante recordar que, aunque los usuarios tienen el control inicial sobre lo que publican, no siempre consideran las implicaciones de compartir información a través de las redes sociales.

Los peligros de las redes sociales se presentan en 3 momentos clave, primero en el registro del usuario. Segundo, mientras se forma parte de ella. Por último, cuando se da de baja el usuario.

[21] FAYOS GARDÓ, A., & CONDE COLMENERO, P. (2015). Los derechos a la intimidad y a la privacidad en el siglo XXI. Madrid, Dykinson. p. 67-68.
[22] ROIG, A. (2009). E-privacidad y redes sociales. IDP: revista de Internet, derecho y política= revista d'Internet, dret i política, n°9. Barcelona, Universitat Oberta de Catalunya. p. 48.

En el primer momento, según el Estudio de la AEPD y el INTECO se presenta el peligro si no se configura adecuadamente el nivel de privacidad, y se publica información de carácter sensible.

En el segundo momento que ocurre cuando se utiliza la red social, el peligro ocurre en dos sentidos. Primero, respecto el propio usuario por la información expuesta, ya que según el Estudio las redes sociales tienen herramientas de intercambio de información. Segundo, por los datos que se publiquen de terceros, debido a que sólo lo pueden hacer si cuentan con el consentimiento de estos.

Por último, aunque se dé de baja el perfil del usuario, podrá seguir constando todavía datos propios o de terceros.

Por lo anterior, es muy importante que el usuario que se crea un perfil en una red social sea consciente de lo que supone publicar sus datos personales, además de información que sea gráfica o escrita, sobre todo sin leer las condiciones de privacidad de las redes sociales.

Por último, cabe destacar que personas famosas de carácter público, debido al avance de las tecnologías y las redes sociales, la información de determinadas cuestiones relativas a su intimidad, podrían ser publicadas en páginas web de diferentes medios de comunicación, pudiendo agravar el daño producido, vulnerando sus derechos a la intimidad, el honor y sus datos personales.

1.6 La autodeterminación informativa

El derecho a la autodeterminación informativa consiste en la,

> "posibilidad que tiene el titular de los datos personales de controlar quiénes serán destinatarios de éstos y qué uso les darán, y se ejercita genéricamente a través de los derechos de acceso, rectificación y cancelación. Además, ofrece una textura que resulta acorde con los modernos desafíos informáticos, puesto que, abandonando el concepto de intimidad como libertad negativa, permite avanzar hacia una fase activa del proceso de circulación de la información personal brindando protagonismo al interesado al posibilitarle el ejercicio de un adecuado control sobre la misma."[23]

Es destacable mencionar que este derecho fue utilizado por primera vez por el Tribunal Constitucional Federal de Alemania, en la sentencia sobre la Ley del Censo del 15 de diciembre de 1983, facultando a las personas a decidir y consentir de manera informada y libre el uso de sus datos personales por terceros, ante el tratamiento automatizado de estos.

[23] BAZÁN, V. (2005). El hábeas data y el derecho de autodeterminación informativa en perspectiva de derecho comparado. Estudios Constitucionales. 3(2). p. 111.

En la actualidad, en la sociedad contemporánea, donde las tecnologías de la información y comunicación (TICs) son esenciales en la vida diaria, surge la necesidad de controlar la información personal en un mundo interconectado por internet y redes sociales. Sin embargo, la protección de datos va más allá de la intimidad y ha generado debates. Algunos consideran que la autodeterminación informativa es solo un aspecto de la intimidad, mientras que otros la ven como un nuevo derecho fundamental que surge de la evolución tecnológica.

El derecho a la intimidad y la autodeterminación informativa están estrechamente relacionados y son componentes de la privacidad. El primero se refiere a proteger la vida privada y controlar el acceso a la información personal, mientras que el segundo abarca el control sobre la recopilación, uso y divulgación de esos datos, siendo vital en la era digital.

Ambos derechos comparten la facultad de controlar la información personal, pero la autodeterminación informativa abarca una gran diferencia que se traduce en facultades como el acceso, rectificación, cancelación de datos, entre otras, no presentes en el derecho a la intimidad.

Ambos derechos se basan en el respeto por la dignidad humana y buscan salvaguardar la capacidad de las personas para tomar decisiones autónomas y controlar sus vidas en una sociedad cada vez más digitalizada.

1.6.1 La autodeterminación informativa en Chile

Aunque se reconoce la importancia de la autodeterminación informativa respaldada por la Ley N°19.628 que protege los datos personales, en la práctica actual esta protección no ocurre. La falta de una entidad reguladora independiente, similar a la Agencia de Protección de Datos en España, y la debilidad en la defensa de los derechos de las personas para controlar sus datos, sugieren que la ley busca equilibrar intereses estatales y lucrativos más que garantizar el control de datos por parte de los individuos.

En resumen, el derecho a la autodeterminación informativa, tal como se entiende tradicionalmente, con sus facultades para controlar datos personales, no encaja en la Ley N°19.628. Esto se refleja en la falta de protección de los titulares de datos ante el Estado y ante entidades privadas. La carencia de una entidad reguladora independiente y la exclusión de personas jurídicas como sujetos protegidos refuerzan la idea de que la autodeterminación informativa no está incorporada en la ley.

CAPÍTULO 2: Evolución histórica normativa de la protección de datos personales

Antes de realizar un análisis sustantivo de la regulación de la protección de datos personales en Chile establecida en la Ley N°19.628, es necesario realizar un recorrido histórico normativo de las primeras leyes sobre la protección de datos personales en el mundo.

2.1 Evolución Histórica Mundial

Las leyes de protección de datos personales surgieron en los años 70, actualmente, tanto los países de la Unión Europea (UE), Estados Unidos (EE.UU), Asia y Oceanía cuentan con legislación sobre protección de datos. Este fenómeno normativo se ha extendido globalmente debido al aumento de la capacidad de almacenamiento y recuperación de información, así como al uso generalizado de la informática y las telecomunicaciones.

La protección de datos personales se ha asociado comúnmente con la protección de la privacidad frente a terceros. En el pasado, los datos personales eran protegidos de diversa manera en distintos países, aunque no se reconocía como una institución autónoma. En su lugar, se ofrecía cierta protección a través de disposiciones legales que a menudo resultaban ambiguas o poco elaboradas.

La protección de los datos personales se menciona de forma indirecta por primera vez a nivel internacional en la Declaración Universal de Derechos Humanos de 1948, que subyace del derecho a la intimidad establecido en el artículo 12.

La enunciación anterior, enfatiza que nadie debe ser objeto de interferencias arbitrarias en su vida privada y tiene derecho a protección legal contra ellas. Este derecho a la intimidad está descrito en un sentido estático, y es reconocido en la mayoría de las constituciones.

Por lo anterior, debido al desarrollo tecnológico, el derecho a la intimidad evoluciona desde una concepción cerrada y estática a una abierta y dinámica debido a los avances tecnológicos, reconociendo en este nuevo ámbito la necesidad de protección de los datos personales, incorporando nuevos mecanismos de protección, como el ámbito constitucional.

Alemania y Suecia fueron los pioneros en el campo de la protección de datos personales, y gradualmente otros países de Europa Occidental se unieron a esta tendencia regulando esta área. A nivel mundial, la tendencia ha sido abordar la protección de datos a través de la vía legislativa, mientras que otros países lo hicieron por la vía constitucional.

2.1.1 Primera Generación de leyes

Entre los años 1960 y 1970, es más concreta su protección, ya que por primera vez se transforma en una "institución legal". Las primeras leyes sobre protección de datos personales son en Alemania en el Estado de Hesse y más tarde en Suecia de 1973 que refleja la preocupación de la época sobre el uso de sistemas de información. Alemania y Suecia son los precursores en la materia de regular la protección de datos personales.

A) Alemania

En 1970 se promulga la ley sobre tratamiento de datos personales del Land de Hesse, en la República Federal de Alemania,

> "mediante la cual se pretendía brindar protección a las personas naturales ante la amenaza que representaba el tratamiento informatizado de datos nominativos por las autoridades y administraciones públicas del Estado, los municipios y entidades locales rurales, así como las demás personas jurídicas de derecho público y agrupaciones sujetas a la tutela estatal. A efectos de asegurar el cumplimiento de sus previsiones, la ley creaba el Comisario de Protección de Datos, al cual garantizaba independencia para el desempeño de sus funciones, cuales eran velar por la observancia de los preceptos de la propia ley y cuantos otros hicieren referencia al trato de los datos de los ciudadanos."[24]

Posteriormente, en Alemania, la Ley Federal de Protección de Datos de 1977 estableció normas para la protección de datos en sectores público y privado. La ley requiere que las instituciones implementen medidas técnicas y organizativas adecuadas para cumplirla. Se crean regímenes normativos específicos para cada sector, y se introducen innovaciones como el Comisario de Protección de Datos, el derecho de bloqueo para los titulares de datos, y sanciones penales e infracciones relacionadas con el tratamiento de datos

B) Suecia

Fue publicada en 1973 la Data Lag, Suecia fue el primer Estado en contar con una ley que cubriera a la vez los bancos de datos del sector público y privado.

[24] SILVA, A. C. (2003). Autodeterminación informativa y leyes sobre protección de datos. Revista Chilena de Derecho Informático, (3). p. 57.

"El modelo sueco de un sistema de registro masivo fue diseñado precisamente para dar nuevos derechos a los particulares afectados, y para imponer nuevas responsabilidades a las organizaciones del sector, fueran éstas públicas o privadas"[25].

La ley sueca requería un registro público de bancos de datos personales en relación con personas físicas procesados por medios automatizados. Estos bancos de datos necesitaban una autorización previa de la autoridad de control, conocida como Datainspektionen, que representa al Ombudsman, una figura legal que vela por el cumplimiento de la ley en los países escandinavos.

El modelo sueco de protección de datos se caracteriza por establecer un registro central de bancos de datos en el país. La autoridad de protección de datos es la única entidad con la capacidad de autorizar a los responsables de estos bancos de datos a manejar información sensible. Los individuos tienen el derecho de conocer qué datos las organizaciones tienen sobre ellos y verificar si se han creado ficheros en su nombre. También tienen el derecho de acceder a sus ficheros y solicitar la corrección de información incorrecta. La ley incluye un catálogo de infracciones que pueden ser sancionadas penalmente, con multas y penas de prisión como posibles consecuencias.

Debido al gran control en la normativa sueca, se le califica en el derecho comparado como modelo de heterocontrol. Esto, ya que existe autorización previa al funcionamiento de bases de datos que han debido de ser mitigadas a través de la adopción de un sistema de notificación e inscripción registral, siendo esta de responsabilidad de la autoridad de control nacional.

La primera legislación se enfocó en la protección de las bases de datos mediante la implementación de restricciones como sistemas de autorización y previa inspección. También se establecieron entidades administrativas encargadas de garantizar el cumplimiento de la normativa, con poderes de fiscalización tanto en la creación de la base de datos como durante su funcionamiento.

2.1.2 Segunda generación de leyes

Posteriormente, debido a los grandes progresos en la informática, se avanza a una segunda generación de leyes. Estas fijan menos trabas para la constitución de bases de datos, por otra parte, le dan al titular de los datos mayores facultades, tales como información, acceso, rectificación y cancelación. Se regula y se dan mayores garantías a los datos sensibles. Estas buscan mejorar la calidad de transmisión de datos. Se delimita el derecho de la autodeterminación informativa, a través de la tutela

[25] DRESNER, S. H. (1994). Panorama de la legislación europea sobre protección de datos personales. Informática y derecho: Revista iberoamericana de derecho informático, (6). p. 390.

y el reconocimiento de los derechos de acceso y control de informaciones. Estas leyes son la Privacy Act de Estados Unidos y la Ley Francesa relativa a la Informática y Libertades.

A) Privacy Act of 1974

> "Establece un código de prácticas justas de información que rige la recopilación, el mantenimiento, el uso y la difusión de información sobre personas que se mantiene en los sistemas de registros de las agencias federales. Un sistema de registros es un grupo de registros bajo el control de una agencia de la cual se recupera información por el nombre del individuo o por algún identificador asignado al individuo"[26].

Esta legislación busca principalmente proteger la privacidad de las personas en sistemas de información federales, y también se aplica al sector privado cuando trabaja para entidades públicas. Regula la recopilación, almacenamiento, uso y divulgación de datos, ya sea en formato digital o manual. La ley establece que los datos de la administración federal solo se pueden revelar con el consentimiento del individuo, a menos que existan razones de orden público. Los titulares de datos tienen derecho a acceder a sus registros, obtener copias y solicitar cambios. También se prevé un proceso de revisión administrativa para casos de negativas de rectificación, junto con una revisión judicial si es necesario.

B) Ley Francesa de 1978 sobre "Informática, Ficheros y Libertades"

Tal como señala en su artículo 1, la informática deberá estar al servicio de los ciudadanos, no deberá atentar la identidad humana, ni a los derechos del hombre, ni a la vida privada, ni a las libertades individuales o públicas. La legislación original regulaba el manejo automatizado de datos personales de personas naturales realizado por personas naturales o jurídicas de derecho público y privado.

El titular puede ejercer los derechos de rectificación y cancelación, y en caso de que el organismo tratante de los datos se niegue, recae la carga de la prueba en éste. La ley impone al organismo la corrección de los registros de oficio y la notificación a terceros a quienes se les transmitió datos modificados.

La ley señala que existe un ejercicio del derecho de acceso por medios indirectos en 2 ámbitos: Primero, "tratándose de datos médicos, deberá procederse por mediación de un profesional de la medicina"[27]. Segundo, datos que afectaren a la seguridad del Estado, defensa o seguridad públicas, se procede mediante la Comisión. Además, la ley impide tomar decisiones judiciales, administrativas o

[26] PRIVACY ACT OF 1974. (16 de junio de 2014). Justice.gov. Recuperado el 13 de mayo de 2023, de https://www.justice.gov/opcl/privacy-act-1974.
[27] SILVA, A. C. (2003). Autodeterminación informativa y leyes sobre protección de datos. Revista Chilena de Derecho Informático, (3). p. 59-60.

privada de las personas basadas únicamente en el tratamiento automatizado de datos. También, establece un catálogo de infracciones y sanciones penales.

Por último, la ley francesa se diferencia de las anteriores leyes descritas, ya que esta contempla un organismo de control, este organismo es la Commission Nationale de I'Informatique et des Libertés, el cual se encarga de velar por la aplicación de la ley, recibir reclamaciones de los agraviados y es dotado de potestad reglamentaria.

Estas legislaciones marcaron un cambio importante en la protección de datos al pasar de centrarse en la regulación de las bases de datos a centrarse en los propios datos. Se diseñaron regímenes jurídicos diferenciados según la naturaleza de los datos y se otorgaron mayores derechos a los titulares de datos para asegurarse de que se traten de manera legal y adecuada.

2.1.3 Tercera generación de leyes

La tercera generación de leyes, debe afrontar el uso sistemático de equipos computacionales, diversas técnicas legislativas, y la insuficiente protección de los datos sensibles, esto porque la transmisión de información automatizada sin precedentes, puede afectar derechos fundamentales, lo cual hace necesaria una evolución a la protección de datos personales extendiéndola a la nueva dinámica ya descrita, con énfasis en precaver riesgos involucrados en la transmisión internacional de datos personales. Esta generación de leyes tiene el objetivo de armonizar y unificar los principios fundamentales y la regulación de datos personales.

A) Convenio 108

> "El Convenio n.º 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal fue el primer instrumento internacional jurídicamente vinculante adoptado en el ámbito de la protección de datos. Tiene como fin garantizar a cualquier persona física el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona. Con el Protocolo que ha modificado el Convenio se pretende ampliar su ámbito de aplicación, aumentar el nivel de protección de los datos y mejorar su eficacia."[28]

[28] LA PROTECCIÓN DE LOS DATOS PERSONALES. (s/f). Europa.eu Recuperado el 15 de mayo de 2023, de https://www.europarl.europa.eu/factsheets/es/sheet/157/la-proteccion-de-los-datos-personales

El Convenio es el principal tratado internacional sobre protección de datos personales. Aunque fue desarrollado por el Consejo de Europa, una vez que está en vigencia, permite que Estados que no son miembros del Consejo de Europa sean invitados por el Comité de Ministros del Consejo de Europa a unirse a él.

Este Convenio otorga un:

> ”marco legal con principios y normas concretas para prevenir la recolección y el tratamiento ilegal de datos personales, datos que son utilizados tanto por gobiernos y sector privado. Estos principios deberán ser recogidos y posteriormente incluidos en las legislaciones nacionales, preservando la calidad de los datos, su legalidad, periodo de conservación, seguridad de los datos personales, derechos de acceso, entre otros.”[29]

El Convenio 108 tiene como objetivo principal regular el procesamiento automatizado de datos de personas naturales. Va más allá de la legislación nacional al buscar armonizar y unificar las leyes europeas existentes desde la década de 1980, y también inspirar nuevas regulaciones europeas. Se trata de una normativa comunitaria que aborda la proliferación de leyes nacionales, facilitando su armonización.

El Convenio regula el almacenamiento de datos personales en el sector público y privado hasta su eliminación, cuando se realiza mediante medios informáticos. Permite a los Estados miembros extender sus disposiciones opcionalmente a grupos de personas, con o sin personalidad jurídica, y a datos personales procesados sin automatización. También supervisa el flujo internacional de datos personales, buscando garantizar una protección equivalente en la legislación para quienes participan en su transferencia. Además, establece un principio de auxilio mutuo entre los Estados parte.

Finalmente, el Convenio 108 obliga a los Estados parte a adoptar en su derecho interno las medidas necesarias para dar cumplimiento a los principios fundamentales de protección de datos que describe el Convenio. Los casos relevantes son los de España y Reino Unido.

B) Recomendación del Consejo relativa a las directrices que regulan la protección de la privacidad y los flujos transfronterizos de datos personales

La OCDE aprueba el 23 de septiembre de 1980 esta “Recomendación”, que tiene principios muy similares a los que se recogen en el Convenio 108 del Consejo de Europa, ya que fueron los mismos

[29] BARRIOS, V. (2018). Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de datos de Carácter personal y su Protocolo Adicional Relativo a las Autoridades de Control a los Flujos Transfronterizos de Datos. Biblioteca del Congreso Nacional de Chile. p. 2.

especialistas que concurrieron a la redacción de uno y otro documento, el texto de "Recomendación" no es obligatorio, pero se reconoce su importancia en las empresas transnacionales. Esta fórmula proposiciones que establecen principios a los que debe sujetarse el tratamiento de datos susceptibles de ser adoptado en el derecho interno.

C) Principios rectores para la reglamentación de los ficheros computarizados de datos personales

Estos principios son adoptados en la Asamblea General de las Naciones Unidas en su resolución 45/95, de 14 de diciembre de 1990. El objetivo de esta resolución es facilitar la incorporación en la normativa interna de cada Estado. La resolución adoptada contiene una serie de principios relativos a las garantías mínimas que deberían de preverse en la legislación nacional: 1) Principio de la ilicitud y lealtad, 2) Principio de exactitud, 3) Principio de finalidad, 4) Principio de acceso a la persona interesada, 5) Principio de no discriminación, 6) Facultad de establecer excepciones, 7) Principio de seguridad, 8) Control y sanciones, 9) Flujo de datos a través de las fronteras, 10) Campo de aplicación.

Campo de aplicación de los principios:

> "Los presentes principios deberían aplicarse en primer lugar a todos los ficheros computadorizados, tanto públicos como privados y, por extensión facultativa y a reserva de las adaptaciones pertinentes, a los ficheros manuales. Podrían tomarse disposiciones particulares, igualmente facultativas, para extender la aplicación total o parcial de estos principios a los ficheros de las personas jurídicas, en particular cuando contengan en parte información sobre personas físicas."[30]

La Resolución 45/95 establece la aplicación de los principios rectores a los ficheros de organizaciones internacionales gubernamentales que almacenan datos personales. Esto se aplica en general, aunque se permiten adaptaciones para tener en cuenta las diferencias entre los ficheros internos de gestión de personal y los ficheros externos relacionados con terceras personas vinculadas a la organización.

Toda organización debe nombrar a una autoridad que estatutariamente sea competente para velar por la correcta aplicación de estos principios rectores.

[30] PRINCIPIOS RECTORES PARA LA REGLAMENTACIÓN DE LOS FICHEROS COMPUTADORIZADOS DE DATOS PERSONALES Adopción: Asamblea General de la ONU Resolución 45/95, 14 de diciembre de 1990 Las modalidades de aplicación de los reglamentos relativos a los ficheros computadorizados de datos personales se dejan a la libre iniciativa de cada Estado con sujeción a las siguientes orientaciones: A. PRINCIPIOS RELATIVOS A LAS GARANTÍAS MÍNIMAS QUE DEBERÍAN PREVERSE EN LA LEGISLACIÓN NACIONAL. (s/f). Gob.mx. Recuperado el 20 de mayo de 2023, de http://www.ordenjuridico.gob.mx/TratInt/Derechos%20Humanos/OTROS%2015.pdf

Finalmente, existe una cláusula humanitaria, la cual prevé una excepción a estos principios cuando el fichero tiene por finalidad la protección de los derechos humanos y libertades fundamentales de la persona, o prestar asistencia humanitaria.

D) Data Protection Act de 1984

Esta legislación adoptada por el Reino Unido es compleja y abarca disposiciones generales junto con regulaciones sobre la inscripción y supervisión de usuarios de datos y oficinas de servicios informáticos. También incluye varios anexos que tratan sobre los principios de procesamiento y su interpretación, el proceso de recurso, la entrada y registro de lugares cerrados.

La ley inglesa de 1984 sobre el tratamiento de datos personales, aplican sus disposiciones tanto al sector público como al privado, a pesar de limitarse a los datos objeto de un procesamiento automatizado. Existen diversos mecanismos de control, adoptando códigos de conducta y el recurso a reglamentación especial, ambos se relacionan con las funciones de la autoridad de control, el "Registrer".

El "Registrer" es la entidad responsable de supervisar el registro de datos y garantizar el cumplimiento de la ley. También se encarga de recibir quejas, asistir a interesados y aplicar medidas cautelares. Se establece un "Data Protection Tribunal" para revisar las decisiones del "Registrer", con la opción de recurrir a tribunales ordinarios. La ley británica de 1984 está relacionada con el Convenio 108, ya que el "Registrer" facilita la cooperación internacional para cumplir con dicho convenio.

Además, cabe mencionar la situación de la Ley Orgánica 2/1992 de Regulación del Tratamiento Automatizado de los Datos de carácter personal" (LORTAD), adoptada en España en 1992, que constituye gran relevancia e influencia para la actual Ley Chilena N°19.628.

E) Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de carácter personal (LORTAD)

La LORTAD se debe a un doble objetivo: Primero, obedece un mandato constitucional del artículo 18.4. Segundo, obedece al mandato del artículo 4 del Convenio de Estrasburgo para la protección de las personas con respecto al tratamiento de los datos de carácter personal.

El texto de la LORTAD se halla integrada por una Exposición de Motivos, 48 artículos distribuidos en 7 Títulos, 3 disposiciones adicionales, una disposición transitoria, una disposición derogatoria y 4 disposiciones finales. En su estructura normativa pueden distinguirse dos sectores básicos: 1) Una parte general o dogmática dedicada a la proclamación de la libertad en la esfera informática en la pluralidad de sus facultades y manifestaciones. 2) Una parte especial u orgánica.

La LORTAD presenta una serie de aspectos positivos como la definición de los principios básicos, el reconocimiento y tutela jurídica de la libertad informática.

Establece como principio básico de su regulación, el requisito del consentimiento de la persona a la que se refieren los datos de carácter personal sometidos a tratamiento automatizado. El simple consentimiento del afectado es necesario y se exige para los demás datos de carácter personal generales de una persona física.

> "La LORTAD fijaba los principios relativos al tratamiento de los datos personales: calidad, información, consentimiento, datos especialmente protegidos, datos de salud, deber de secreto, seguridad y cesiones, así como los derechos de las personas: acceso, rectificación, cancelación e impugnación de valoración."[31]

Por otra parte, la LORTAD se complementó con dos normas reglamentarias: El Real Decreto 1332/1994 del 10 de junio que desarrolla diversas disposiciones; y el Real Decreto 994/1999 del 11 de junio, sobre las medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal. En la actualidad ambas están derogadas.

Por último, la LORTAD crea la "Agencia de Protección de Datos" la cual se encarga de sancionar con multas a los que transgreden estos derechos, esto también en relación con el cumplimiento del Convenio 108. Pese a que Chile es influenciado por la LORTAD, no cuenta con una institución fiscalizadora como la "Agencia de Protección de Datos" u otra institución similar.

F) El Reglamento General de Protección de Datos (GDPR) (Reglamento 2016/679)

El Reglamento General de Protección de Datos,

> "es un reglamento por el que el Parlamento Europeo, el Consejo de la Unión Europea y la Comisión Europea tienen la intención de reforzar y unificar la protección de datos para todos los individuos dentro de la Unión Europea (UE). También se ocupa de la exportación de datos personales fuera de la UE. El objetivo principal del GDPR es dar control a los ciudadanos y residentes sobre sus datos personales y simplificar el entorno regulador de los negocios internacionales unificando la regulación dentro de la UE. Cuando el GDPR surta efecto, sustituirá a la Directiva de protección de datos (oficialmente Directiva 95/46 / CE) de 1995. El Reglamento fue adoptado el 27 de abril de 2016. Se convierte en ejecutivo a partir del 25 de

[31] SEMPERE, J. (2012). XX Aniversario de la LORTAD: 20 años de Protección de Datos. Diario Jurídico Español, Madrid. Recuperado el 26 de mayo de 2023, de https://www.diariojuridico.com/xx-aniversario-de-la-lortad-20-anos-de-proteccion-de-datos/

mayo de 2018 tras una transición de dos años y, a diferencia de una directiva, no obliga a los gobiernos nacionales a aprobar ninguna legislación habilitante, por lo que es directamente vinculante y aplicable."[32]

El ámbito de aplicación del GDPR se relaciona con la protección y libre circulación de datos personales, derogando la Directiva 95/46/CE. Este reglamento se aplica a datos personales que son tratados de forma total o parcialmente automatizada, así como a datos personales que se procesan de manera no automatizada, pero están destinados a ser incluidos en un archivo. Sin embargo, excluye ciertos tipos de tratamientos, como actividades personales o domésticas exclusivamente, actividades bajo el Tratado de la Unión Europea (capítulo 2 del título V) y el tratamiento de datos en actividades no cubiertas por el derecho de la Unión Europea. El ámbito de aplicación territorial del GDPR se establece en su artículo 3.

El objetivo del Reglamento es fortalecer los derechos fundamentales en la era digital y fomentar la actividad económica. Aporta claridad a las regulaciones aplicables a las empresas y entidades públicas en el mercado único digital e incluye nuevos tipos de datos para su protección, como los identificadores en línea. Además, establece que los datos personales pseudónimos pueden estar sujetos a las normas de la GDPR, dependiendo de su nivel de identificabilidad.

La GDPR busca dar a las personas más control sobre cómo se utilizan sus datos personales La GDPR busca reforzar la legislación sobre protección de datos e introducir medidas de aplicación más estrictas. Además, se busca dar a las empresas un entorno jurídico más simple y claro para operar, haciendo que la ley de protección de datos sea uniforme en todo el mercado, ya que el objetivo principal de la GDPR es unificar los principios de protección de datos de la UE.

El GDPR establece 10 requisitos clave para el tratamiento de los datos personales: 1) Tratamiento legal, leal y transparente; 2) Limitación del fin, datos y almacenamiento; 3) Derechos de los interesados: Acceso, oposición, corrección, eliminación y transferencia de datos; 4) Consentimiento expreso y documentado; 5) Registro de violación de seguridad y notificación en 72 horas; 6) Privacidad en el diseño de sistemas y procesos; 7) Responsabilidad en la Transferencia de datos; 8)Evaluación del impacto en la protección de datos; 9)Nombrar un delegado de protección de datos (DPO); y 10) Certificación.

Por otro lado, cabe mencionar que el artículo 51 de la GDPR establece que cada Estado miembro establecerá que sea responsabilidad de una o varias autoridades independientes (autoridad de control)

[32] GDPR: LO QUE DEBES SABER SOBRE EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS. (s/f). Powerdata.Es. Recuperado el 27 de mayo de 2023, de https://www.powerdata.es/gdpr-proteccion-datos

supervisar que se aplique el Reglamento. Además, dispone que las autoridades de control cooperarán entre sí y con la Comisión Europea.

Por último, el artículo 84 de la GDPR establece que los Estados miembro establecerán las normas en materia de otras sanciones aplicables a las infracciones del Reglamento, en concreto las infracciones que no se sancionen con multas administrativas del artículo 83, adoptando todas las medidas necesarias para el cumplimiento del Reglamento, las sanciones deben ser efectivas, proporcionadas y disuasorias.

2.2 El reconocimiento Constitucional de la protección de datos personales

Es importante mencionar las primeras consagraciones constitucionales del derecho a la protección de datos personales como derecho fundamental.

La protección de datos personales se ha ido incorporando progresivamente en las constituciones europeas y latinoamericanas, ya sea de manera expresa o tácita. Ahora abordaremos las primeras Constituciones que reconocieron el derecho a la protección de datos personales en el ámbito constitucional europeo y latinoamericano.

2.2.1 Reconocimiento Constitucional en Europa

A) La Constitución portuguesa de 1976

> "La Constitución pionera en este campo fue la portuguesa de 1976, que en un detallado art. 35 reconoce los derechos de acceso y rectificación, y prohíbe el tratamiento de datos personales sensibles salvo para fines estadísticos, así como la asignación de un número identificativo único"[33].

En resumen, en el apartado 1 del artículo 35 "Utilización de la informática", establece que todos los ciudadanos tienen derecho a tener conocimiento lo que contengan los registros mecanográficos acerca de sus datos personales y de la finalidad del destino de tal información, pudiendo exigir la rectificación y actualización de los datos. Luego, en el apartado 2, se describe que no se podrá utilizar la informática para el tratamiento de los datos referentes a convicciones políticas, religiosas o vida privada, excepto si se trata de la elaboración por fines estadísticos de datos no identificables. Finalmente, en su apartado 3, existe una prohibición de atribuir a los ciudadanos un número nacional único.

[33] PASCUAL, P (2017). La génesis del derecho fundamental a la protección de datos personales. [Tesis Doctoral, Universidad Complutense de Madrid]. p. 260. https://docta.ucm.es/rest/api/core/bitstreams/6ac257e3-656a-4aed-a4f2-c3b855c77cd7/content

B) La reforma constitucional austriaca de 1978

La Ley federal austriaca de protección de datos, conocida como "Datenschutzgesetz" y promulgada el 18 de octubre de 1978, establece en su apartado primero un auténtico derecho fundamental a la protección de datos "Grundrecht auf Datenschtz". Este derecho se considera una disposición constitucional, tal como se indica explícitamente en la ley.

En resumen, dicha ley establece que, las personas tienen derecho a exigir y hacer valer en juicio la confidencialidad de sus datos personales y a proteger su vida privada y familiar. Solo se permiten limitaciones si se protegen intereses legítimos de otros o si tales limitaciones tuvieren su base en leyes que fueren necesarias en virtud de las razones que se mencionan el artículo 8, segundo párrafo, del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, pese a estas limitaciones, se debe darle prioridad a la confidencialidad de los datos personales. También se garantiza el derecho a exigir información sobre el procesamiento de datos cuando se elaboren datos acerca de la persona con ayuda de medios automáticos. Además, las personas tendrán derecho a solicitar la rectificación y cancelación de datos incorrectos o indebidos. El derecho a la protección de datos se aplica tanto a entidades públicas como privadas, y se hará valer a través de la jurisdicción ordinaria en caso de entidades de derecho público que utilicen formas de derecho privado.

C) La Constitución española de 1978

En el apartado de los derechos fundamentales, se reconoce en el artículo 18.4 una norma relacionada a la protección de datos personales, la cual señala que la ley limitará el uso de la informática para garantizar el honor, y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio legítimo de sus derechos. Los principios de protección establecidos se aplican únicamente a los ciudadanos españoles. La protección de extranjeros dependerá de acuerdos de reciprocidad o convenios internacionales, en relación con los ciudadanos de los Estados que los hayan suscrito y aceptado. La constitución española tomó como ejemplo la Constitución portuguesa para la redacción de este artículo.

> "En concreto, la STC 94/1998, señaló que nos encontramos ante un derecho fundamental a la protección de datos por el que se garantiza a la persona el control sobre sus datos, cualesquiera datos personales, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados; de esta forma, el derecho a la protección

de datos se configura como una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquél que justificó su obtención."[34]

2.2.2 Reconocimiento Constitucional en América Latina

Los países latinoamericanos comenzaron a percibir los riesgos del avance de las tecnologías y el riesgo de la informática, por ello, se empezó a reconocer el derecho a la protección de datos personales.

A) Brasil

La Constitución de Brasil de 1988 en el artículo 5 deriva el derecho de la protección de datos personales, se fundamenta a partir de las siguientes disposiciones. Artículo 5, LXXII, regula el Habeas Data, mientras que el artículo 5, X, se protege el derecho a la intimidad y la vida privada, por otra parte, en el artículo 5, XII, aborda el secreto de las comunicaciones, y el artículo 5, XXXII, garantiza la protección del consumidor en un contexto de crecimiento del mercado de datos.

B) Colombia

La Constitución de Colombia en 1991 reconoce constitucionalmente en el artículo 15 el derecho de la protección de datos personales, estableciendo que todas las personas tienen derecho a la intimidad, el buen nombre y a controlar la información sobre ellas. El Estado debe respetar y proteger estos derechos. Además, se garantiza el derecho de las personas a acceder, actualizar y rectificar los datos que se han recopilado sobre ellas en bases de datos y archivos de entidades privadas y públicas. En todo el proceso de recolección, tratamiento y circulación de datos se deben respetar las libertades y garantías establecidas en la Constitución.

C) Perú

La Constitución de Perú en 1993 reconoce constitucionalmente el derecho de la protección de datos personales en su artículo 2.6, estableciendo que toda persona tiene derecho a que los servicios informáticos, ya sea computarizados o no, privados o públicos, no suministren informaciones que afecten a la intimidad familiar y personal.

En Latinoamérica encontramos en diversas normas de rango constitucional el derecho de la protección de datos personales, además de las anteriormente descritas, entre ellas se encuentran las constituciones de Paraguay en 1992 y Argentina en 1994.

[34] SINOPSIS ARTÍCULO 18. Constitución Española. (s/f). Congreso.es. Recuperado el 30 de mayo de 2023, de https://app.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=18&tipo=2

CAPÍTULO 3: La protección de datos personales

3.1 Concepto

La protección de datos personales, la doctrina lo define como:

> "la protección jurídica de las personas en lo que concierne al tratamiento de sus datos de carácter personal, o de otra forma, el amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento, para confeccionar una información que, identificable con él, afecta a su entorno personal, social o profesional, en los límites de su intimidad, incide directamente en un derecho fundamental de elevado contenido. Son elementos característicos de la definición constitucional de este derecho fundamental los derechos del afectado a consentir sobre el uso y la recogida de sus datos personales y a saber de los mismos"[35].

Entonces, la protección de datos personales se puede describir como el conjunto de normas y principios que regulan el tratamiento de datos personales en todas sus etapas, es decir, la recolección, almacenamiento, circulación, publicación y transferencia nacional e internacional.

En cuanto a la expresión "protección de datos", se da a entender que se protegen los datos, pero dicha interpretación es errónea, ya que lo que se busca proteger es al titular de los datos personales.

Con el objetivo de una mejor compresión de la definición, es necesario distinguir dos conceptos que usualmente son confundidos en el lenguaje cotidiano, "dato" e "información".

Dato se define como cualquier hecho manifestado bajo una fórmula convencional adecuada para su comunicación, interpretación o tratamiento, ya sea por el ser humano o por medios informáticos.

En cambio, la información se puede definir como el conjunto de dato organizado, ordenados y reordenados utilizables. La información se refiere a los datos que se han procesado, analizado e interpretado para obtener un significado y un contexto.

Otros conceptos que son importantes distinguir, son los denominados archivos, base de datos y bancos de datos. Estos conceptos unos estructuran a los otros, de forma ascendente como se puede apreciar a continuación.

[35] CONDE ORTIZ, C. (2005). La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad. Madrid, Dykinson. p. 29.

Primero, archivo o fichero se refiere a un conjunto de documentos y registros relacionados con una persona, empresa o entidad en particular, que se mantienen organizados y almacenados para su posterior uso y consulta. Los archivos pueden contener una amplia variedad de información.

Segundo, una base de datos es un conjunto organizado de información relacionada según sus atributos comunes, en función de posibles requerimientos.

Por último, banco de datos es un conjunto organizado de base de datos que pueden ser accesibles mediante medios electrónicos o informáticos.

Entonces, se puede entender como dato personal toda información relacionada con una persona natural identificada o identificable, como su nombre, número de identificación personal, dirección, teléfono, correo electrónico, datos bancarios, información de salud, filiación política, credo religioso, operaciones comerciales, etc.

En resumen, cuando nos referimos a la protección de datos personales, no solo nos referimos al elemento "dato", sino que a todos los demás elementos que se originan con la combinación de los datos, como lo es la "información", y dicha información se estructura en distintos niveles, en forma ascendente: archivos, base de datos y banco de datos, todo esto en referencia a una persona determinada.

Por su parte, en Chile, el derecho a la protección de datos personales se define como "el conjunto de normas jurídica destinada a asegurar al individuo el respeto de sus derechos y libertades fundamentales y, especialmente, el respeto a su intimidad ante el cada vez más frecuente tratamiento automatizado de los datos de carácter personal"[36], desde esta perspectiva, se entiende que el derecho a la protección de datos personales establece que toda persona tiene el control y la facultad de decidir sobre la recopilación, uso y almacenamiento de sus datos personales, esto con el fin de proteger la dignidad humana y la autonomía de las personas, por otra parte, este derecho establece obligaciones para las entidades que tratan los datos personales para garantizar su uso adecuado. Asimismo, la Ley N°19.628 define el derecho de protección de datos personales como el derecho que tienen las personas naturales sobre el control y protección de los datos que las identifica o permite identificarlas. Este derecho puede abarcar cualquier tipo de dato relacionado con una persona, como su nombre, dirección, número de teléfono, datos bancarios, etc.

[36] NAVARRETE, S. (2008). La protección de datos personales en Chile y la Ley 19.628. [Tesis de licenciatura, Universidad Austral de Chile]. p. 35. http://cybertesis.uach.cl/tesis/uach/2008/fjn321p/doc/fjn321p.pdf

3.2 Naturaleza jurídica

La naturaleza jurídica del derecho a la protección de datos es compleja y multifacética, y ha sido objeto de debate en distintas jurisdicciones a nivel mundial, ya que su reconocimiento y protección depende de las normas y regulaciones establecidas en cada jurisdicción.

Por lo general, se considera que el derecho a la protección de datos es un derecho fundamental que está relacionado con otros derechos, como el derecho a la privacidad, la libertad y la autonomía individual. Además, en diversos ordenamientos jurídicos este derecho puede ser ejercido y protegido ante los tribunales competentes, además existen leyes que establecen principios y procedimientos necesarios para garantizar su adecuada protección.

En el ámbito jurídico, el derecho a la protección de datos se ha reconocido en distintas normas a nivel global. En la Unión Europea, por ejemplo, el derecho a la protección de datos está protegido por el Reglamento General de Protección de Datos (GDPR), dicho reglamento establece normas para el tratamiento de datos personales por parte de entidades públicas y privadas.

En otras jurisdicciones, el derecho a la protección de datos se reconoce como un derecho fundamental de carácter constitucional, como ocurre en Colombia.

Por otro lado, el derecho a la protección de datos es un derecho de carácter autónomo que deriva de la dignidad humana y la libertad individual, este derecho reconoce la facultad de las personas para controlar y decidir sobre sus propios datos personales, y establece obligaciones para aquellas entidades que tratan datos personales. En efecto, el derecho a la protección de datos es un derecho que protege la privacidad y la intimidad de las personas, garantizando la autonomía de las personas para controlar su información personal, siendo esencial para garantizar el equilibrio entre los derechos individuales y los intereses generales de la sociedad.

Por su parte, en Chile, la naturaleza jurídica es de derecho fundamental de carácter constitucional, el cual es inherente a todas las personas con el fin de proteger su intimidad y vida privada, así se establece en el artículo 19 N°4 de la Constitución. Antes de la publicación de la Ley N°21.096, la doctrina lo consideraba incorporado en la Constitución en el artículo 19 N°4 como un aspecto de la privacidad.

Por lo tanto, en Chile,

> ”antes de este reconocimiento expreso, el derecho a la protección de datos personales se había entendido como parte del contenido iusfundamentalmente protegido del derecho al respeto

y protección de la vida privada, establecido en el artículo 19 N°4 de la Constitución. Así lo había argumentado la doctrina y la jurisprudencia mayoritaria."[37]

Con la Ley N°21.096 del 16 de junio de 2018, reforma constitucional, se reconoció como derecho fundamental en la Constitución de la República de Chile el derecho a la protección de datos personales, y a la vez se le reconoce como derecho independiente del derecho al respeto y protección de la vida privada, facultando a las personas a controlar sus datos personales y la capacidad para disponer sobre los mismos, es por ello que se modifica el artículo 19 de la Constitución, agregando al numeral 4° el derecho a la protección de datos personales, añadiendo que el tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley.

3.3 La protección de datos personales como derecho fundamental

A inicios de la década de 1980 diversos países, entre ellos Chile, enfrentaban el problema del desarrollo de las tecnologías de la información, en cuanto al procesamiento de los datos de las personas automatizado, aplicándose para tomar determinadas decisiones que afectaban a las personas, vulnerando sus derechos fundamentales. Lo anterior, se puede observar en una serie de vulneraciones como son la denegación de créditos, denegar el acceso a determinados colegios, limitar el arrendamiento de viviendas, denegación de seguros de salud y trabajos.

Lo que sucedía en los hechos era que alguien,

"prácticamente imposible de identificar, recogía datos de múltiples fuentes, los analizaba y a partir de ellos creía saber algo acerca de una determinada persona (nadie sabía qué), para luego tomar decisiones a su respecto en base a lo anterior. Con ello se comenzaron a limitar o derechamente negar derechos y, en definitiva, afectar los proyectos de vida de cada quien, dada la relativa invisibilidad del fenómeno. Ni siquiera había a quien pedir explicaciones por ello. Aunque el afectado por estas decisiones advirtiera ciertas inconsistencias o arbitrariedades, tampoco tenía a quien recurrir para saber quién o cómo se había tomado la decisión, qué información tenían respecto de él y, menos todavía, quién o quiénes la habían tomado."[38]

[37] CONTRERAS, P. (2020). El derecho a la protección de datos personales y el reconocimiento de la autodeterminación informativa en la Constitución chilena. Estudios constitucionales, vol 18(2). p. 89.
[38] DONOSO, L, y REUSSER, C. (2021). Protección de Datos Personales. Santiago. Ed, Academia judicial de Chile. p. 11.

Por lo anterior, se justifica la protección de los datos personales como derecho fundamental, los cuales son derechos que se pueden considerar naturales y esenciales, tienen un carácter básico debido a la importancia para el desarrollo de la persona humana.

Tal como se señalaba, estamos ante una sociedad cada vez más tecnologizada, en donde la información es muy relevante, en la que dependen muchas prestaciones y servicios para la satisfacción de las personas, por ello la importancia de proteger los datos con el fin de promover el desarrollo. Al mismo tiempo, el derecho a la protección de datos personales se funda en la dignidad humana, cuyo valor es inherente e intrínseco que posee toda persona como ser humano.

El derecho a la protección de datos personales se considera un derecho fundamental porque está intrínsecamente relacionado con la privacidad, intimidad, la libertad y la dignidad humana. En un mundo cada vez más digitalizado, la recolección y el uso de datos personales se ha convertido en una práctica cotidiana, y en muchos casos se realiza sin el consentimiento de las personas afectadas, el tratamiento inadecuado de los datos personales, pueden resultar en la vulneración de su privacidad, su dignidad humana y derechos fundamentales, por ello, el derecho a la protección de datos personales se ha establecido como un mecanismo esencial para proteger la privacidad y la libertad individual, con el fin de contrarrestar la discriminación y el abuso por parte de los individuos o instituciones que manejan los datos personales.

Cabe añadir, que el derecho a la protección de datos personales está intrínsecamente relacionado con otros derechos fundamentales como lo son el derecho a la libertad de expresión, la libertad de información, la libertad de asociación, la privacidad, la honra, el honor, la propia imagen, la intimidad, entre otros. Por, ejemplo si los datos personales se recolectan y se utilizan de manera indebida, esto puede afectar la capacidad de las personas para expresarse libremente o para asociarse con otros de manera segura y confidencial, además de denegarles a las personas de forma injustificada determinados derechos que se describen en los párrafos anteriores en este mismo apartado.

En conclusión, el derecho fundamental de la protección de datos personales le da un mecanismo de protección a los derechos de las personas, controlando el flujo de informaciones que conciernen a cada persona, permitiendo a las personas como titulares de sus datos personales, manejar el contenido de los datos. El derecho a la protección de datos personales se considera un derecho fundamental porque protege la dignidad humana de las personas, su privacidad y autonomía, por ende, este derecho es esencial para mantener el equilibrio entre los derechos individuales y los intereses generales de la sociedad.

3.4 Titularidad de los datos personales

Los titulares del derecho a la protección de datos personales son las personas cuyos datos personales están siendo procesados, recopilados, almacenados, utilizados, compartidos, difundidos, ya sea por el sector privado o el sector público. En otras palabras, son todas aquellas personas identificadas o identificables a quien corresponden los datos personales, y tienen el derecho a que se le respete su privacidad y se garantice la protección de sus datos personales.

En términos generales, cualquier persona tiene derecho a la protección de sus datos personales, y este derecho se encuentra reconocido en diversos tratados internacionales de derechos humanos, como la Declaración Universal de Derechos Humanos que se infiere a través de la interpretación del artículo 12, la Convención Americana sobre Derechos Humanos que se deriva de la interpretación del artículo 11, la Carta de los Derechos Fundamentales de la Unión Europea, regulando la protección de los datos personales en el artículo 8, en la que toda persona tiene derecho a la protección de sus datos personales que le corresponden, además establece que dichos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley, en la que toda persona tiene derecho a acceder a los datos recogidos que le corresponden y a su rectificación, por último se señala que el respeto de las normas quedará sujeto al control de una autoridad independiente. Entonces, el derecho a la protección de datos personales se encuentra reconocido en diversos tratados internacionales como los anteriormente mencionados, entre otros. Asimismo, muchos países tienen regulaciones específicas que establecen la protección de los datos personales de las personas, definiendo quiénes son sus titulares de derecho y las obligaciones de las entidades que recopilan y procesan los datos personales.

Por último, la doctrina inicialmente señalaba que los titulares de los datos personales sólo correspondían a las personas físicas o naturales, pero los titulares del derecho a la protección de datos personales, puede extenderse a personas jurídicas, como las empresas, aunque esto depende de la jurisdicción y la ley aplicable de cada país.

Por su parte, en Chile los titulares de los datos personales que son objeto de tratamiento son aquellas personas naturales a la que hacen referencia los datos personales, así se establece en el artículo 2 letra ñ) de la Ley N°19.628.

3.5 ¿Existe un derecho de propiedad sobre los datos?

En principio, la titularidad de los datos personales no dice relación alguna con la propiedad sobre los datos personales, la titularidad en Chile como se establece en el artículo 2 letra ñ) de la Ley 19628

solo es la relación que se da entre la persona natural identificada o identificable y los datos de carácter personal a que se refieren.

Se discute en la doctrina si es posible configurar un derecho de propiedad sobre los datos, para resolver dicha discusión se recurre a las normas contenidas en la Constitución y el Código Civil.

Según nuestra legislación actual,

> ”se concluyó que los datos como entidades independientes de su contenido y dimensión física, no son susceptibles de ser protegidos por un derecho de dominio, porque no pueden ser clasificados como cosas corporales o incorporales según las normas del *Código Civil*. En consecuencia, no existe una relación de propiedad o especie de propiedad entre una persona y los datos, según las normas del derecho común. Del mismo modo, cuando se estudió desde el punto de vista constitucional, específicamente el art. 19 n.° 24 de la Constitución, se sostuvo que no es posible argumentar que existe un derecho de propiedad sobre bienes inmateriales diversos a los ya regulados en el *Código Civil*, porque la doctrina interpreta esta disposición como una mera restricción a las cosas incorporales que, al mismo tiempo, son bienes susceptibles de apropiación.”[39]

La legislación chilena en vez de establecer un derecho de propiedad sobre los datos se enfoca en la protección de la privacidad y los derechos de los titulares de los datos personales, estableciendo la ley una serie de principios y normas para el tratamiento adecuado de los datos. No obstante, es importante mencionar que los datos personales pueden ser objeto de regulación y control por parte de los titulares, quienes tienen derecho a conocer, acceder, rectificar, cancelar y oponerse al tratamiento de sus datos.

3.6 Importancia de la protección de los datos personales

El avance tecnológico ha traído beneficios y exposición a la sociedad debido a la interconexión global y el papel fundamental de los datos en la economía moderna. Los datos personales son valiosos para el desarrollo económico, la innovación y la ventaja competitiva de las empresas en una sociedad altamente tecnológica e interconectada, un ejemplo de esto es el comercio electrónico definido como:

> “el vasto conjunto de actividades con finalidad mercantil que se desarrolla mediante el uso de sistemas de procesamiento de datos y de comunicaciones sin que exista un contacto físico directo entre quien oferta un bien o un servicio y quien lo demanda la denominación cubre no

[39] JARA, N. (2021). El derecho de propiedad sobre los datos. *Revista chilena de derecho privado*, (TEMATICO). p.139.

solamente actos comerciales directos, como la compraventa o alquiler, sino también acciones preparatorias o conexas como la publicidad o mercadeo."[40]

Asimismo, los datos de las personas están en permanente tratamiento por medio de empresas privadas y organismos públicos, con múltiples propósitos, siendo dichos datos una fuente importante de control y poder, debido a la mercantilización de dichos datos que constantemente se comercializa por parte de empresas o personas que se dedican a su venta. Este mercado de datos surge debido a que tanto el Estado como a los particulares les es fundamental conocer la información de las personas contenida en sus datos personales para así poder tomar decisiones, ya sea para el desarrollo de políticas públicas, marketing, publicidad, para conocer el estado financiero de una persona, salud, nivel educacional, nacionalidad, patrimonio o cualquier otra información que se obtenga a partir de dichos datos.

No obstante, el avance tecnológico también plantea riesgos para los derechos individuales al comprometer el honor, la privacidad, la imagen y los datos personales. Esto puede tener impactos culturales, económicos y sociales, ya que los individuos pueden tener dificultades para conocer qué entidad almacena sus datos y con qué propósito,

> "la gente tiene miedo de que sus datos sean usados incorrectamente, violando no solo su bolsillo sino también su privacidad. Una consecuencia de todos esos resultados es la conclusión de que la falta de consentimiento de las personas para la utilización de sus datos es habitual"[41].

Entonces, la falta de regulación adecuada puede llevar a la dispersión no controlada de datos personales en internet. La transferencia internacional de datos, facilitada por la interconexión global, puede resultar en que la información personal termine en cualquier parte del mundo, lo que constituye un riesgo para los derechos fundamentales como la protección de datos.

Debido a esta realidad y la exposición al peligro, se hace necesario legislar en leyes que protejan los datos personales. Los derechos de la protección de datos personales deben contener entre sus disposiciones, primero limitar y supervisar el uso de la tecnología en el tratamiento de datos personales. Segundo, conciliar el legítimo interés del Estado y los particulares por recolectar información, con los derechos de los titulares de los datos personales. Asimismo, la protección de datos debe resguardar la intimidad o autodeterminación de las personas frente al uso de datos personales por parte del Estado o de particulares, garantizándole a los titulares de los datos personales la debida protección y confiriéndole a los titulares control sobre sus datos, entre otros elementos con el objetivo de proteger los datos

[40] NÚÑEZ, E. (2007). La importancia de la protección de datos de carácter personal en las relaciones comerciales. Aproximación al Derecho venezolano. Revista de derecho privado. p. 117-118.
[41] TRAVIESO, J (2016). Protección de datos personales y tecnología. En busca del paraíso perdido. Revista tribuna internacional, vol 5, n°9. p. 111.

personales de las personas. Por ejemplo, en una ley de protección de datos personales podríamos proteger derechos tales como el de la intimidad, el honor, la propia imagen, entre otros que pueden verse afectados por el tratamiento indebido de datos.

En conclusión, ha cobrado relevancia la protección de los datos personales, haciendo necesaria su regulación debido a los avances tecnológicos originando una gran recolección, almacenamiento, asociación, transferencia e interconexión de datos personales. Las regulaciones normativas en diversos ordenamientos jurídicos a nivel global han debido de ir evolucionando producto del desarrollo y avance tecnológico.

Todo lo anterior, ha preocupado a la doctrina nacional por la vulneración de la vida privada de las personas, derivando con ello en el reconocimiento del derecho a la protección de datos personales, no sólo con una normativa especial, como es el caso de la Ley N°19.628, sino que también como derecho fundamental como es el caso de nuestra Constitución, derecho establecido en el artículo 19 N°4, protegido ante posibles vulneraciones a través de un recurso de protección, y la creación de garantías procesales como la acción de habeas data con el fin de proteger los datos personales.

CAPÍTULO 4: Tratamiento y protección de los datos personales en la Ley N°19.628

4.1 Origen de la Ley N°19.628

A) Debate Parlamentario previo a la Ley N°19.628: La Moción del ex Senador Eugenio Cantuarias

La Ley N°19.628 tiene origen en una moción parlamentaria presentada por el ex Senador Eugenio Cantuarias Larrondo el 5 de enero del año 1993. La tramitación del proyecto de ley excedió los 6 años. La orientación del proyecto de ley cambió profundamente, originando la regulación del tratamiento de datos personales, cuestión que para gran parte de la doctrina nacional y extranjera constituye una manifestación del derecho a la intimidad o la vida privada. La moción del ex Senador Cantuarias, sobre protección "civil" de la vida privada,

> "nunca pretendió ser una ley de protección de datos personales o nominativos. Antes, muy por el contrario, el ex Senador consignó expresamente que sólo buscaba resaltar algunos principios fundamentales para aproximarse al tema y que la materia debía ser abordada en otro proyecto más acabado. Su moción, fundada en una ley similar española, era un proyecto de ley sobre protección "civil" de la vida privada, bien jurídico que debía ser resguardado ante lo que él llamaba 11 intromisiones ilegítimas."[42]

El ex Senador Cantuarias buscaba llenar un vacío existente en la legislación civil respecto al derecho a la intimidad o vida privada, ya que no existía un cuerpo legal que desarrollara las disposiciones del artículo 19N° 4 y 5 de la Constitución de 1980. Además, se tuvo en consideración como parámetros de orientación los instrumentos internacionales de derechos humanos, entre los cuales se considera la Declaración Universal de Derechos Humanos de 1948 y la Convención Americana sobre Derechos Humanos de 1969, entre otros instrumentos internacionales. En concreto, la idea del proyecto era generar un estatuto de la privacidad, teniendo como base la Ley Orgánica española N°1 del 5 de mayo de 1982, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, con el objetivo de entregar a las personas una protección civil efectiva de estos derechos frente a agravios de terceros.

[42] LEIVA, R. J. J. (1999). Dominios, marcas y comercio electrónico en internet: anexo: la nueva ley chilena sobre la no protección de datos personales, Nº 19628 del 28 de agosto de 1999. Informática y derecho: Revista iberoamericana de derecho informático, (30). p. 379.

El proyecto de ley contenía 26 artículos, se distribuían en 5 Títulos: Título I sobre disposiciones generales, Título II sobre protección de datos (artículos 8 a 13), Título III de las intromisiones ilegítimas, Título IV de las acciones civiles, y Título V sobre tribunal competente y procedimiento.

B) Proyecto aprobado por el Senado en octubre de 1995

El texto de la moción fue reducido a 16 artículos ordenados en 4 Títulos que se describirán a continuación:

El Título I, sobre las disposiciones generales (artículos 1 a 4): Aludiendo a garantías o derechos diferentes como son la privacidad, el honor y la imagen, estableció el ámbito de aplicación de la ley, "el respeto y protección a la vida privada y a la honra de la persona y su familia". Además, se refiere al alcance legal del concepto de "la vida privada". También, estableció que las sentencias judiciales no podían fundarse en intromisiones ilegítimas. Por último, consagró una obligación del secreto estadístico.

El Título II, "de la protección de datos" (artículos 5 a 9): Señalaba algunos principios Fundamentales de la no desviación del fin por la cual se procesan los datos, los datos almacenados tienen la obligación de ser informados, con derecho de acceso o conocer cuáles son los datos procesados, además de rectificarlos, aclararlos, actualizarlos, completarlos o suprimirlos, finalmente estableció un derecho a la indemnización de perjuicios.

El Título III (artículos 10 al 12): Definió lo que constituía como una intromisión ilegítima en la vida privada.

El título IV (artículos 13 al 16): Describe acciones, procedimientos y competencias para conocer los casos de infracciones a la ley, siendo obligatorio indemnizar incluso el daño moral.

C) Modificaciones incorporadas al proyecto de ley en la Cámara de Diputados

La Cámara de Diputados en un segundo trámite constitucional, señaló que lo más relevante del proyecto aprobado por el Senador eran las normas relacionadas sobre protección de datos personales. Por lo tanto, en vez de aprobar un texto simple y genérico tanto en el fondo como en su forma, se intentó elaborar una normativa legal integral, y se buscó promulgar en Chile una ley de protección de datos, similar a la ley francesa de 1978 y española de 1992. En este sentido, el proyecto modificado por la Cámara de Diputados es muy distinto al texto aprobado por la Cámara del Senado. El nuevo texto ahora es exclusivamente sobre protección de datos personales, siendo presentado en 1998 al Senado para un tercer trámite constitucional.

Debido a que este proyecto fue aprobado en el Senado y modificado por la Cámara de Diputados, se decidió remitir a la comisión de Constitución, Legislación, Justicia y Reglamento del Senado, la que en su informe final rechazó el proyecto remitido por la Cámara de Diputados.

D) Debate en Comisión Mixta

Producto de las diferencias entre ambas Cámaras del Congreso durante la tramitación del proyecto, se formó una Comisión Mixta integrada por miembros de ambas Cámaras, resultando de su informe final el texto definitivo de la Ley N°19.628, que fue publicado en el Diario Oficial el 28 de agosto de 1999 y entró en vigor 60 días después. Asimismo, la ley contenía un artículo transitorio que otorga un año de plazo a los organismos públicos que realizaban el tratamiento de datos personales, con el objetivo de que puedan adecuarse a lo establecido en la ley.

Cabe tener en consideración, que la Ley N°19.628 no regula todos los aspectos de la vida privada de las personas. La Ley N°19.628 solo regula de manera muy específica el tratamiento de datos personales en registros o bancos de datos, y protege la vida privada de las personas sólo cuando ésta es afectada por el tratamiento de sus datos personales.

4.2 Estructura de la Ley N°19.628

La Ley N°19.628 fue publicada en el Diario Oficial el 28 de agosto de 1999 y se estructura de la siguiente manera compuesta por 24 artículos permanentes y 3 transitorios, contenidos en 7 títulos:

Título preliminar: Contiene disposiciones generales, como el ámbito de aplicación, y se describen una serie de definiciones jurídicas en los artículos 1, 2 y 3.

Título I “De la utilización de datos personales” (artículos 4-11): Es el título más extenso, y se refiere a los datos, su tratamiento y a las responsabilidades de las personas dedicadas en esta actividad.

Título II “De los derechos de los titulares de datos” (artículos 12-16): En este título se configuran los derechos de acceso, cancelación y bloqueo de los datos, además del procedimiento para reclamar judicialmente el respeto a los datos personales.

Título III “De la utilización de datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial” (artículos 17-19): Se les otorga una regulación especial.

Título IV “Del tratamiento de datos por los organismos públicos” (artículos 20-22)

Título V “De la responsabilidad por las infracciones a esta ley” (artículo 23)

Título Final: Modifica el Código Sanitario (artículo 24).

Por último, existen 3 artículos transitorios. El primero, dispone 2 periodos de gracia legal, uno de 60 días contados desde la publicación en el Diario Oficial, por ende, la ley entró en vigor en octubre de 1999. El otro, señala un plazo de un año contado desde la misma fecha de publicación, para que se cumpla con lo establecido en el artículo 22 relacionado a la creación de un registro de bancos de datos personales a cargo de organismos públicos. El segundo artículo transitorio amplia los derechos que confiere esta ley a los titulares de datos personales registrados en bancos creados con anterioridad a la entrada en vigor de esta ley. Por último, el tercer artículo extiende la vigencia del Decreto Supremo N°950 del Ministerio de Hacienda de 1928 que regula al Boletín de Informaciones Comerciales, en todo lo que no sea contario a la nueva Ley N°19.628.

En este apartado, se realizará un análisis de la Ley N°19.628 tomando en consideración su marco conceptual y ámbito de aplicación, los principios que informan el tratamiento de los datos personales, los derechos de su titular, entre otras materias relevantes en relación con el tratamiento de los datos personales y su protección.

La protección de datos personales se encuentra en nuestro país en la Ley N°19.628, y con la ley 21.096 publicada el 16 de junio de 2018 en el Diario Oficial, se consagra constitucionalmente el derecho a la protección de datos personales, proyecto de reforma constitucional que fue ingresado el 11 de junio de 2014 originándose mediante una moción parlamentaria.

La idea del proyecto consiste en reconocer como derecho fundamental que el ciudadano tenga la facultad de controlar sus datos personales, disponerlos y decidir sobre estos. Por ello, mediante esta reforma constitucional,

> "se modifica el artículo 19 de la Constitución Política de la República que consagra las garantías constitucionales de las personas, para agregar en su numeral 4º el Derecho a la Protección de los Datos Personales. De este modo en la Carta Fundamental, se reconoce la protección de los datos personales, y además señala que el tratamiento y protección de estos datos, se efectuará en la forma y condiciones que determine la ley."[43]

En el final del numeral se hace referencia a que el tratamiento y la protección de los datos personales se efectuará en la forma y condiciones que determine la ley, entre estas leyes, se remite a la Ley N°19.628.

[43] MICROJURIS.COM CHILE. (18 de junio de 2018). Ley Nº 21.096 consagra constitucionalmente el Derecho a la Protección de datos personales. Noticias legales. Microjuris al Día Chile. Recuperado el día 5 de junio de 2023, de https://aldiachile.microjuris.com/2018/06/18/ley-no-21-096-consagra-el-derecho-a-la-proteccion-de-datos-personales/

4.3 Modificaciones a la Ley N°19.628

La Ley N°19.628 ha sido objeto de varias modificaciones, en la que muchas de ellas se originaron para remediar una serie de abusos y vulneraciones que sufrían las personas debido al tráfico de datos personales por parte de empresas, o producto de que la misma ley ha sido insuficiente. En general gran parte de las modificaciones tienen relación con el tratamiento de datos de carácter económico. Sin embargo, ninguna de las modificaciones, también llamadas "Leyes Parche", solucionó de forma integral las deficiencias de la Ley N°19.628, por lo tanto, aún persisten falencias estructurales en la ley.

A) Ley 19.812

Se publicó el 13 de junio de 2002. La Ley 19.812 modificó los artículos 16, 17 y 18 de la Ley N°19.628. Primero, se modificó el inciso quinto del artículo 16, aumentando el monto de la multa de 10 a 50 Unidades Tributarias Mensuales cuando se cometiera una infracción a los artículos 17 y 18, sin embargo, el monto de la multa a nuestro juicio no genera un incentivo suficiente para respetar la norma, ya que sigue siendo un monto bajo. Segundo, se agregó al inciso primero del artículo 17, la siguiente frase: "Se exceptúa la información relacionada con los créditos concedidos por el Instituto Nacional de Desarrollo Agropecuario a sus usuarios"[44] . Tercero, se agregó al inciso segundo del artículo 17, que "no podrá comunicarse la información relacionada con las deudas contraídas con empresas públicas o privadas que proporcionen servicios de electricidad, agua, teléfono y gas"[45]. Por último, se reemplazó los incisos primero y segundo del artículo 18, estableciendo que en ningún caso se podrán comunicar los datos de la información financiera del artículo 17 que se relacionen con una persona identificable o identificada después de transcurrir 5 años desde que se hizo exigible la obligación. Además, se añadió, que no se puede comunicar los datos que se refieran a obligaciones que a la fecha de publicación de la ley hayan sido extinguidas por otro modo legal o hayan sido pagadas.

También, esta ley modificó el Código del Trabajo, esta ley buscó hacer efectivo el derecho a la no discriminación consagrado constitucionalmente, estableciendo el principio de no discriminación, con el fin de eliminar la discriminación que ocurría al solicitarle a los postulantes a un puesto de trabajo su historial financiero condicionando su contratación, por ello se introduce un nuevo inciso 6 al artículo 2 estableciendo que ningún empleador podrá sujetar la contratación de trabajadores por falta de obligaciones de carácter financiero, económico, comercial o bancario, que puedan ser comunicadas por los bancos de datos personales o responsables de registros conforme a la ley, por ello el empleador no podrá exigir para la contratación de trabajadores declaración, ni certificado, excepto los trabajadores con

[44] LEY N° 19.812, MODIFICA LA LEY N°19.628, SOBRE PROTECCIÓN DE LA VIDA PRIVADA. (11 de junio de 2002). Artículo 1, numeral segundo. Diario Oficial de la República de Chile, Santiago.
[45] Artículo 1, numeral tercero de la Ley 19.812.

labores gerenciales, de representación, administrativas y los que tengan a su cargo la recaudación, administración o custodia de valores o fondos de cualquier naturaleza. Sin embargo, "esta reforma no terminó con la perniciosa práctica de solicitar a los postulantes a un puesto de trabajo que presenten su historial financiero y de esta forma discriminar a quienes tengan deudas pendientes."[46]

B) Ley 19.899

Publicada el 18 de agosto de 2003 en el Diario Oficial, introdujo cambios significativos en relación con las nóminas de los deudores morosos de los fondos solidarios de crédito universitario. Se estableció en su artículo 13 bis de esta ley que, estas nóminas se consideran públicas sin que les haya sido ni les sea aplicable lo establecido en la Ley 19.812. En síntesis, la ley 19.899 permite la comunicación de la morosidad de deudas de crédito universitario.

La Ley 19.899 permitió la publicación completa de la lista de deudores morosos, en contraposición a las limitaciones establecidas por la llamada ley Dicom, que regulaba qué deudas podían ser divulgadas y cuáles no. Esta modificación fue influenciada por decisiones judiciales favorables a Dicom.

De acuerdo con el diario de sesiones de la Cámara de Diputados, en la sesión del 13 de agosto de 2004, se buscaba que las deudas de este tipo de obligaciones no estuvieran sujetas a la prohibición de divulgación una vez que hubieran cumplido el plazo establecido por la ley para la morosidad. En cambio, se buscaba mantener la publicación de las listas de estos deudores hasta que su deuda fuera completamente saldada, debido a las condiciones favorables para los deudores previstas por el legislador en este tipo de créditos.

C) Ley 20.463

Esta ley se origina debido a que,

> "se reconoció que los empleadores no respetaban lo previsto en el Código del Trabajo y que solicitaban un "informe Dicom" a las personas que postulan a un trabajo, desechando aquellas que presentaban información adversa. Por lo anterior, la Ley 20.463, de 2010, modificó el artículo 17 de la Ley N°19.628, suspendiendo la comunicación de la información comercial de las personas cesantes."[47]

[46] VIOLLIER, P. (2018). El Estado de la protección de datos personales en Chile. Derechos Digitales. p. 18.
[47] DONOSO, L, y REUSSER, C. (2021). Protección de Datos Personales. Santiago. Ed, Academia judicial de Chile. p. 80.

En síntesis, la ley prohíbe la comunicación de información sobre morosidades de personas cesantes.

Entonces, la ley publicada el 25 de octubre de 2010 prohíbe a los administradores de bases de datos financieros el tratamiento de datos relacionados con deudas de personas naturales durante períodos de desempleo. Sin embargo, esta restricción solo aplica a la publicación e intercambio de información financiera sobre morosidad generada durante el desempleo, no afectando las deudas anteriores derivadas de la falta de empleo. Además, si una persona no está cubierta por un seguro de cesantía, es responsabilidad del deudor certificar su situación de desempleo ante el Boletín Comercial.

Esta reforma tuvo un impacto limitado, ya que solo aborda las deudas generadas durante el período de cesantía, sin considerar las obligaciones previas que no pudieron ser cumplidas debido al desempleo. Además, se establece un proceso complicado para aquellos que no están cubiertos por un seguro de cesantía, quienes deben realizar el trámite por sí mismos para ejercer su derecho durante un período de tres meses, renovable una vez, lo cual es insuficiente. Esto puede perjudicar a las personas que no pueden pagar sus obligaciones de manera permanente.

D) Ley 20.521

La ley publicada el 23 de julio de 2011 prohíbe la evaluación de riesgo comercial que no estén respaldadas en información objetiva relacionada con el estado financiero de las personas. En caso de incumplimiento, los afectados tienen derecho a reclamar compensación por los daños sufridos y solicitar la eliminación inmediata de la información no objetiva de las bases de datos. Sin embargo, esta normativa tiene una debilidad significativa, ya que su texto breve no define claramente qué se entiende por "información objetiva", lo que limita su efectividad legal. De hecho, es necesario recurrir a la historia de la ley para comprender el contexto en el que se promulgó, debido a la brevedad de su texto.

E) Ley 20.575

La ley publicada el 17 de febrero de 2012 representa una de las modificaciones más significativas de la Ley N°19.628. Esta ley se divide en dos partes. Los artículos 1 a 6 establecen un cuerpo normativo independiente, mientras que los artículos 7 a 8 modifican la Ley N°19.628.

> "El principal mérito de esta ley fue consagrar en la legislación chilena el principio de finalidad. Analizado más adelante. Vale la pena mencionar que esta legislación tuvo el propósito expreso de evitar el abuso en el tratamiento de datos personales por parte de distintas entidades, al punto que la prensa la denominó como "Ley DICOM" (El Mostrador, 2012), en alusión a las

prácticas de quienes utilizaban los datos consignados en Equifax, heredera de la antigua empresa dedicada al tratamiento de datos e información de carácter comercial."[48]

El objetivo principal de esta ley era proteger los derechos de los consumidores, incluso si tenían deudas pendientes, ya que estar en el Boletín Comercial les cerraba muchas oportunidades más allá de solicitar préstamos y créditos bancarios. Se buscaba evitar el abuso y el lucro en el tratamiento de datos personales por parte de diversas entidades. En marzo de 2012, el diputado Felipe Harboe denunció ante el SERNAC que la empresa EQUIFAX "permite la compra de antecedentes comerciales a través de Internet, pidiendo sólo el RUT y el código verificador. Asimismo, Equifax continuaría entregando antecedentes comerciales a universidades y empresas, a pesar de que la ley 20.575 lo prohíbe"[49].

F) Ley 21.214

La ley publicada el 28 de febrero de 2020 modifica la Ley N°19.628, sobre protección de la vida privada, con el fin de prohibir que se informe sobre las deudas contraídas para financiar la educación en todos sus niveles. Este artículo único de esta ley incorpora en el inciso segundo del artículo 17 de la Ley N°19.628, sobre protección de la vida privada, un nuevo inciso que amplía las restricciones de comunicación de información relacionada con deudas. Se establece que:

"No podrá comunicarse la información relacionada con las deudas contraídas con empresas públicas o privadas que proporcionen servicios de electricidad, agua, teléfono y gas", lo siguiente: "tampoco 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 Nº 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;"."[50]

G) Ley 21.504

La ley publicada el 10 de noviembre de 2022 modifica la Ley N°19.628, estableciendo prohibición de informar deudas contraídas para financiar servicios y acciones de salud en la Ley

[48] VIOLLIER, P. (2018). El Estado de la protección de datos personales en Chile. Derechos Digitales. p. 19.
[49] SERNAC INVESTIGARÁ DENUNCIA CONTRA EQUIFAX POR INCUMPLIMIENTO DE LEY DICOM. (s/f). SERNAC: Noticias. Recuperado el 10 de junio de 2023, de https://www.sernac.cl/portal/604/w3-article-6696.html
[50] LEY N° 21.214, MODIFICA LA LEY N°19.628, SOBRE PROTECCIÓN DE LA VIDA PRIVADA, CON EL OBJETO DE PROHIBIR QUE SE INFORME SOBRE LAS DEUDAS CONTRAÍDAS PARA FINANCIAR LA EDUACIÓN EN CUALQUIERA DE SUS NIVELES. (24 de febrero de 2020). Artículo Único. Diario Oficial de la República de Chile, Santiago.

N°19.628. Este artículo único de esta ley introduce una modificación al inciso segundo del artículo 17 de la Ley N°19.628, sobre protección de la vida privada,

> "con el objeto de prohibir que se informe sobre las deudas contraídas para financiar servicios y acciones de salud, a continuación de la expresión "en cualquiera de sus niveles;", lo siguiente: "ni las deudas contraídas con prestadores de salud públicos o privados y empresas relacionadas, sean instituciones financieras, casas comerciales u otras similares, en el marco de una atención o acción de salud ambulatoria, hospitalaria o de emergencia sean éstas consultas, procedimientos, exámenes, programas, cirugías u operaciones;"."[51]

4.4 Principios de los datos personales en la Ley N°19.628

A) Principio de la libertad en el tratamiento de datos personales

La ley no busca prohibir el tratamiento de datos personales, "antes bien procura someterlo a un régimen jurídico que conjugue de un lado el interés de quienes requieren el procesamiento de ellos con una garantía a los derechos de aquellos a quienes se refieren"[52]. Según el artículo 1 de la Ley N°19.628, se establece que toda persona tiene la capacidad de procesar datos personales. Sin embargo, esta ley establece tres condiciones que deben cumplirse para conciliar los intereses de todas las partes involucradas: 1) El tratamiento debe realizarse de acuerdo con la ley, 2) solo se permite para fines legales, y 3) siempre se debe respetar plenamente el ejercicio de los derechos fundamentales de los titulares de los datos, así como las facultades reconocidas por la ley.

B) Principio de la información y consentimiento del titular

Con el objetivo de proteger el derecho de los individuos a controlar su información personal,

> "la ley establece que el tratamiento de datos personales solo puede realizarse mediando una autorización expresa por parte de la ley –entendida como la propia Ley N°19.628, u otra– o del titular de los datos. En este último caso, dicha persona debe ser informada sobre el propósito del almacenamiento de sus datos y su eventual publicación, y la autorización debe realizarse de forma expresa y por escrito. Dicha autorización puede ser revocada sin necesidad de causa justificada, pero ello no tiene efecto retroactivo"[53].

---

[51] LEY N°21.504, ESTABLECE PROHIBICIÓN DE INFORMAR DEUDAS CONTRAÍDAS PARA FINANCIAR SERVICIOS Y ACCIONES DE LA SALUD EN LA LEY N°19.628. (4 de noviembre de 2022). Artículo Único. Diario Oficial de la República de Chile, Santiago.

[52] CERDA, A. (2012). Legislación sobre protección de las personas frente al tratamiento de datos personales. Santiago, Centro de Estudios en Derecho Informático, Universidad de Chile. p. 23.

[53] VIOLLIER, P. (2018). El Estado de la protección de datos personales en Chile. Derechos Digitales. p. 21.

Aunque el consentimiento expreso e informado es la regla general para el tratamiento de datos personales, la ley establece en el artículo 4 una serie de excepciones a este principio, dicha regulación se abordará posteriormente. Algunos autores argumentan que estas excepciones son tan amplias que, en la práctica, la regla general se convierte en la excepción.

C) Principio de finalidad

El principio de finalidad en la Ley N°19.628 fue reforzado por la Ley 20.575, estableciendo que los datos personales solo pueden ser utilizados para los fines para los cuales fueron recopilados. Este principio está relacionado con el consentimiento informado del titular, ya que sería ilegítimo utilizar los datos para otros fines no autorizados.

La ley establece que:

> "los datos personales deben utilizarse sólo para los fines para los cuales hubieren sido recolectados, salvo que provengan o se hayan recolectado de fuentes accesibles al público. Los entes que traten datos podrán establecer procedimientos automatizados de transmisión, siempre que se cautelen los derechos de los titulares y la transmisión guarde relación con las tareas y finalidades de los organismos participantes. La Ley señala que el receptor de los datos personales transmitidos sólo puede utilizar los datos personales para los fines que motivaron dicha transmisión."[54]

Para abordar el problema de entidades comerciales que proporcionaban certificados financieros de personas a cambio de tarifas, la Ley 20.575 limita la comunicación de datos económicos, financieros, bancarios o comerciales a comercios establecidos y entidades de evaluación de riesgo comercial, únicamente para el proceso de crédito. Además, prohíbe exigir esta información en procesos de selección personal, admisión educativa, atención médica de emergencia o postulación a cargos públicos, así se establece en el artículo 1 de la Ley 20.575.

D) Principio Calidad de los datos

Este principio se establece en el artículo 9, inciso segundo de la Ley N°19.628. Este principio implica que la información debe ser precisa, estar actualizada y reflejar fielmente la situación real del titular. Si se incumple esta obligación, el titular tiene el derecho de solicitar la modificación, bloqueo o eliminación de los datos.

[54] GARRIDO, R. (2013). El Habeas data y la ley de protección de datos en Chile. Serie Bibliotecología y Gestión de Información, (83). p. 14.

Para garantizar la idoneidad de los datos personales, es necesario que sean adecuados, pertinentes y no excesivos, es decir, limitados a lo necesario para los fines del tratamiento. Esto se establece en el artículo 9 de la Ley N°19.628, que exige que la información sea precisa, actualizada y refleje la situación real del titular.

Esto implica lo siguiente: 1) la información debe ser precisa y completa; 2) debe estar actualizada, reflejando la situación actual; y 3) debe ser verídica, basada en hechos comprobables. Estas características deben evaluarse en cada caso.

En resumen, la veracidad y exactitud de los datos están condicionadas por la actualidad, lo que significa que los datos deben modificarse para reflejar la situación actual del titular en todo momento.

E) Principio de protección especial de los datos sensibles

El legislador ha establecido una protección especial para los datos personales considerados sensibles debido a su naturaleza. Estos datos incluyen información sobre características "físicas o morales de las personas o circunstancias de su vida privada o íntima"[55], así se establece en el artículo 2 letra g). El tratamiento de estos datos conlleva un mayor riesgo de violación de derechos fundamentales, por lo que el legislador ha impuesto restricciones más estrictas.

En general, está prohibido el tratamiento de datos sensibles, pero existen tres excepciones permitidas por la ley: autorización expresa de la ley, consentimiento del titular de los datos y necesidad de determinar o proporcionar beneficios de salud a los titulares de dichos datos, así se establece en el artículo 10.

F) Principio de seguridad de los datos

La Ley N°19.628 establece en su artículo 11 la obligación del responsable de los registros o bases de datos de proteger los datos personales con diligencia y asumir la responsabilidad por cualquier daño causado. Sin embargo, la ley no especifica los estándares o medidas concretas que deben seguir estos responsables para garantizar la seguridad de los datos. Por lo tanto, corresponde a los tribunales,

> "definir cuándo se han adoptado las medidas apropiadas para el cumplimiento satisfactorio de la obligación impuesta al responsable del banco de datos, para lo cual habrán de atender al estado de desarrollo tecnológico, la naturaleza misma de los datos y los riesgos a que ellos se encuentren afectos. Por su parte, será de competencia del responsable de la base de datos

[55] ROSENDE, H., RABAT, F., & WARNIER, M. (2013). Algunos alcances sobre la protección de los datos de carácter personal. Revista Actualidad Jurídica, Universidad del Desarrollo. p. 210.

acreditar la adopción de medidas de protección adecuadas en el tratamiento de los datos personales."[56]

G) Principio deber de secreto

La ley exige en el artículo 7 que los responsables de los registros o bancos de datos mantengan la confidencialidad de los datos personales obtenidos de fuentes no accesibles al público. Esta obligación persiste incluso después de que dejen de ser responsables de la base de datos, extendiéndose en el tiempo.

H) Principio de Garantías ante la cesión y la comunicación de datos a terceros

A diferencia de otros países, la legislación chilena no aborda específicamente la transferencia transfronteriza de datos, lo que puede limitar su eficacia en la protección de los datos personales. Esto significa que los datos podrían ser enviados a países que no cumplen con el nivel de protección establecido por la Ley N°19.628.

Se permite la transmisión automatizada de datos si se protegen los derechos de los titulares y está relacionada con los propósitos de las entidades involucradas. El responsable del banco de datos receptor evalúa la solicitud, pero la responsabilidad es del solicitante, así se establece en el artículo 5 inciso 3. También se requiere documentar la identificación del solicitante, el motivo y propósito de la solicitud, y el tipo de datos transmitidos.

Estas obligaciones no se aplican cuando los datos se obtienen de fuentes accesibles al público. Además, no se aplican a las transmisiones de datos a organizaciones internacionales en cumplimiento de tratados y convenios internacionales, así se establece en el artículo 5 inciso final. Esto destaca la importancia de que esos tratados y convenios establezcan estándares adecuados de protección de datos personales.

I) Principio de lealtad y licitud del tratamiento de datos

En Chile, existen dos condiciones principales para el tratamiento legítimo de datos personales: la ley y el consentimiento del titular. La lealtad y la licitud son elementos fundamentales en el manejo de datos de terceros, y el responsable del tratamiento debe cumplir con el deber de custodia. Estos principios se aplican en todas las etapas del proceso de tratamiento de datos personales, y deben orientar la interpretación y aplicación de la normativa de protección de datos.

[56] CERDA, A. (2012). Legislación sobre protección de las personas frente al tratamiento de datos personales. Santiago, Centro de Estudios en Derecho Informático, Universidad de Chile. p. 29.

J) Principio de transparencia

El principio de transparencia, respaldado por los artículos 3 y 4 de la Ley N°19.628, requiere que el responsable del tratamiento de datos personales tenga políticas claras y transparentes. Esto implica adoptar medidas para informar al público sobre la existencia de los tratamientos, sus propósitos, los responsables y garantías para los titulares de datos. Además, se debe cumplir con el deber de registro de las actividades de tratamiento y proporcionar información necesaria para obtener el consentimiento.

K) Principio de control

El principio de control establece la necesidad de verificar que el tratamiento de datos personales cumpla con los principios y normas aplicables. Este control puede ser ejercido por "el interesado a través de los derechos que se le reconocen, o a través de una agencia pública o autoridad de control, concebida como un órgano independiente encargado de vigilar la aplicación de las normas de protección de datos"[57].

Las autoridades de control deben contar con atribuciones consultivas y técnicas para asesorar tanto a las autoridades públicas como al sector privado en la aplicación y mejora de la normativa de protección de datos. También tienen poderes de investigación para recopilar la información necesaria en el ejercicio de su función de control.

Además, se les otorgan poderes de intervención, como autorizar tratamientos, impartir instrucciones, bloquear, suprimir o destruir datos, prohibir tratamientos, emitir advertencias o amonestaciones, y remitir casos a los tribunales de justicia u otras autoridades competentes, según corresponda.

Es importante destacar que las autoridades de control también tienen atribuciones jurisdiccionales para conocer y denunciar infracciones a la ley ante la autoridad judicial. Sin embargo, en Chile, la ley prescinde de una autoridad de control que vele por la protección de los datos personales, por ende, el titular puede solo recurrir a los tribunales de justicia a través del recurso de protección o la acción de habeas data solicitando el restablecimiento del imperio del derecho con el objetivo de proteger sus datos personales y solicitar, en el caso de la acción de habeas data las indemnizaciones correspondientes.

[57] DONOSO, L, y REUSSER, C. (2021). Protección de Datos Personales. Santiago. Ed, Academia judicial de Chile. p. 141.

4.5 Ámbito de aplicación de la Ley N°19.628

El ámbito de aplicación no es la protección de la vida privada o la intimidad de las personas, es mucho más limitado y específico,

> "por una parte, un ámbito de aplicación material u objetivo, el cual recae sobre el tratamiento de datos de carácter personal, sea éste automatizado o manual y, por otro lado, un ámbito subjetivo que trata sobre los individuos a quienes se les aplica la ley, a saber: 1) los titulares de los datos, siendo siempre las personas naturales a las que se refieren los datos, lo que excluye a las personas jurídicas según el Art. 2 letra ñ) de la Ley N° 19.628 y 2) el responsable del registro o banco datos, que puede ser una persona natural o jurídica, pública o privada y que le compete las decisiones que se relacionen con el tratamiento de estos datos, en términos de la letra n) del mismo artículo."[58]

El ámbito de aplicación de la ley se establece en el artículo 1, estableciendo que:

> "El tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares se sujetará a las disposiciones de esta ley, con excepción del que se efectúe en ejercicio de las libertades de emitir opinión y de informar, el que se regulará por la ley a que se refiere el artículo 19, N° 12, de la Constitución Política."[59]

En relación con el alcance de aplicación de la ley en términos de los individuos respecto de los cuales es aplicable la ley y el cumplimiento de las obligaciones establecidas, se distingue entre los titulares de los datos y quienes realizan el tratamiento de estos. Los titulares de los datos personales son las personas naturales a las que se refieren los datos personales, excluyendo a las personas jurídicas. Por otro lado, los responsables del registro o banco de datos son las personas naturales o jurídicas, tanto privadas como organismos públicos, que toman decisiones relacionadas con el tratamiento de los datos personales.

[58] KINDLEY, D. (2017). "El régimen de la Protección de Datos Personales en Chile: Análisis comparado, estándares internacionales y revisión crítica. El Derecho al Olvido y su tutela a través de la acción de Habeas Data". [Tesis de licenciatura, Universidad Austral de Chile], Repositorio institucional. p. 27. http://cybertesis.uach.cl/tesis/uach/2017/fjk.51r/doc/fjk.51r.pdf

[59] LEY N° 19.628, SOBRE PROTECCIÓN DE LA VIDA PRIVADA. (18 de agosto de 1999). Artículo 1, inciso primero. Diario Oficial de la República de Chile, Santiago.

4.6 Conceptos fundamentales de la Ley N°19.628

Al conceptualizar y desarrollar el derecho a la protección de datos, surgen otros conceptos esenciales, siendo estos las bases del derecho a la protección de datos, cuyos conceptos relevantes están descritos en el artículo 2 de la Ley.

a) Almacenamiento de datos: La ley en su artículo 2 letra a) señala que es "la conservación o custodia de datos en un registro o banco de datos"[60]. El responsable del banco de datos tiene la obligación implícita de garantizar la seguridad de los datos, como se desprende del término "custodia" utilizado en la definición.

b) La comunicación o transmisión de datos: El artículo 2 letra c) de la Ley señala que es "dar a conocer de cualquier forma los datos de carácter personal a personas distintas del titular, sean determinadas o indeterminadas"[61]. En resumen, se refiere a la cesión a cualquier título de los datos personales. La revelación de datos personales a terceros puede ser realizada de diversas formas, tanto físicas a través de un documento como digitales a través de una red, e incluye la simple visualización de los datos.

c) Fuentes accesibles al público: El artículo 2 letra i) de la Ley establece que son, "los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes"[62]. Los datos son accesibles de forma libre, pero su recopilación y tratamiento deben realizarse legalmente y de acuerdo con las obligaciones establecidas en la Ley N°19.628.

d) El artículo 2 letra k) de la Ley señala que son:

> "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 N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado."[63]

e) Procedimiento de disociación de datos: El artículo 2 letra l) establece que es "todo tratamiento de datos personales de manera que la información que se obtenga no pueda asociarse a persona determinada o determinable"[64]. El procedimiento de disociación de datos tiene como objetivo evitar la asociación de los datos recopilados con personas específicas. La facilidad para lograr este objetivo

[60] Artículo 2, letra a) de la Ley 19.628.
[61] Artículo 2, letra c) de la Ley 19.628.
[62] Artículo 2, letra i) de la Ley 19.628.
[63] Artículo 2, letra k) de la Ley 19.628.
[64] Artículo 2, letra l) de la Ley 19.628.

depende del número de sujetos y de sus características particulares. Como resultado de la disociación de datos, se generan datos estadísticos

f) Registro o banco de datos: La Ley N°19.628 en su artículo 2 letra m) señala que es:

> "el conjunto organizado de datos personales, sea automatizado como las bases de datos electrónicas o manual, como los archivos de papel, y cualquiera sea la forma o modalidad de su creación u organización, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos."[65]

g) Sujetos del tratamiento: Primero, tenemos a los responsables del tratamiento de datos, y estos se subclasifican en responsable del registro o banco de datos establecido en el artículo 2 letra n) de la Ley 19628, es decir, "la persona natural o jurídica privada, o el respectivo organismo público, a quien compete las decisiones relacionadas con el tratamiento de los datos de carácter personal"[66], (almacenamiento, uso y destino de los datos personales).

Todas las personas, tanto naturales como jurídicas, tienen el derecho de llevar a cabo el tratamiento de datos personales, ya sea de forma manual o automatizada, de acuerdo con la ley y para fines legales. Sin embargo, este derecho está sujeto a limitaciones y se debe respetar plenamente los derechos fundamentales de los titulares de los datos y las facultades reconocidas por esta ley.

Cualquier persona, ya sea natural o jurídica, de derecho público o privado, puede realizar el tratamiento de datos personales, siempre y cuando cumpla con los siguientes requisitos:

1)Estar autorizado por la Ley N°19.628, como en el caso del tratamiento de datos personales provenientes de fuentes accesibles al público, el tratamiento realizado por organismos públicos en sus áreas de competencia, o mediante el consentimiento expreso del titular de los datos.

2)Respetar las facultades concedidas a los titulares de los datos personales, como el derecho de acceso, modificación y eliminación, entre otros.

3)La finalidad del tratamiento de los datos personales debe estar permitida por la legislación.

4)Se debe garantizar el pleno ejercicio de los derechos fundamentales de los titulares de los datos personales.

[65] Artículo 2, letra m) de la Ley 19.628.
[66] Artículo 2, letra n) de la Ley 19.628.

Es importante tener en cuenta que la autorización del titular debe ser expresa, informada y por escrito, y puede ser revocada, aunque sin efecto retroactivo.

Por otra parte, tenemos al prestador de servicios de tratamiento, que es el encargado del tratamiento, es una persona natural o jurídica, entidad pública o privada, distinta de la persona responsable, que realiza operaciones de tratamiento de datos personales en nombre y por cuenta del responsable del banco de datos o registro.

Por último, tenemos al interesado, quien es el titular de los datos personales o sujeto de los datos personales, que según el artículo 2 letra ñ) de la ley, esta es "la persona natural a la que se refieren los datos de carácter personal"[67], y son objeto de tratamiento por esta ley, el interesado es el titular del derecho a la protección de datos, además las personas jurídicas no son contempladas como titulares de datos personales, y no se sujetan, ni se protegen mediante esta ley.

La Ley Nº 19.628 establece las definiciones de los conceptos mencionados anteriormente. Es importante destacar que, según su artículo 1, esta ley se aplica al tratamiento de datos personales en registros o bancos de datos por parte de organismos públicos o privados. Esto indica que la regulación abarca tanto a los particulares como a los organismos del Estado. Además, se trata de una ley de carácter general y supletoria.

h) Tratamiento de datos: "está referido a cualquier operación o conjunto de operaciones, sean o no automatizadas, que se aplique a datos de carácter personal, en especial su recogida, conservación, utilización, revelación o supresión"[68].

Por su parte, el artículo 2 letra o) de la Ley N°19.628 conceptualiza con mayor profundidad el concepto, señalando que tratamiento de datos es:

> "cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizados 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 utilizados de cualquier forma."[69]

La ley no se limita a los tratamientos automatizados de datos personales, sino que también abarca los tratamientos manuales de información. Además, la lista de verbos en la definición es solo

[67] Artículo 2, letra ñ) de la Ley 19.628.
[68] DONOSO, L, y REUSSER, C. (2021). Protección de Datos Personales. Santiago. Ed, Academia judicial de Chile. p. 29.
[69] Artículo 2, letra o) de la Ley 19.628.

ejemplificativa, lo que significa que existen otras actividades que pueden considerarse como tratamiento de datos, como la publicación de datos personales en páginas web.

Con respecto al tratamiento de datos es relevante mencionar:

Todas las personas pueden manejar datos personales respetando lo establecido en la ley y para fines permitidos. Se necesita consentimiento explícito de la ley o del titular para tratar datos. No se necesita autorización para tratar datos de fuentes accesibles al público. Se debe mantener en secreto información de personas que trabajan con datos no accesibles al público. Los datos sensibles solo pueden ser tratados en casos autorizados por la ley. Los titulares pueden solicitar información, modificaciones, cancelaciones, bloqueos y eliminaciones de datos. Los organismos públicos pueden tratar datos relacionados con su competencia sin consentimiento, pero cumpliendo los requisitos legales. El responsable del tratamiento de datos debe indemnizar por daños causados por tratamiento indebido.

La aplicación de la ley de protección de datos personales se enfrenta a varios desafíos, como la diversidad de empresas e instituciones que realizan el tratamiento de datos y la amplia variedad de tipos de datos disponibles en el mercado, como registros de salud, crédito, proveedores de internet, compras en línea, registros comerciales, antecedentes criminales, entre otros. Esto ha generado problemas debido a la falta de una legislación sólida en Chile para regular los diversos tipos de bancos de datos existentes.

4.7 Clasificación de los datos personales

La Ley N°19.628, al igual que otras legislaciones internacionales sobre datos personales, proporciona definiciones claras de varios conceptos, entre ellos las diferentes interpretaciones del término "datos".

Al igual que en el derecho comparado,

> "nuestra ley establece diversas categorías de datos, atendiendo al grado de protección que requieren. Así, encontramos a los datos de protección ordinaria, sujetos a la reglamentación general de la ley en cuanto a su tratamiento. Luego hay otros llamados datos de mera identificación. Provenientes generalmente de fuentes accesibles al público, requieren un menor grado de protección pero no por eso pueden considerarse absolutamente inocuos o sin interés. Y finalmente, los datos sensibles, que demandan una mayor protección atendidas sus características propias que exigen que en general se prohíba su tratamiento."[70]

[70] NAVARRETE, S. (2008). La protección de datos personales en Chile y la Ley 19.628. [Tesis de licenciatura, Universidad Austral de Chile]. p. 58. http://cybertesis.uach.cl/tesis/uach/2008/fjn321p/doc/fjn321p.pdf

Por su parte, Cerda señala que:

> "Un "dato" es una unidad básica de información; ahora cuando la información que porta el dato es relativa a una persona determinada o susceptible de serlo, se denomina dato personal o dato nominativo, esto es, una unidad de información que se predica de persona determinada o determinable."[71]

En la ley se definen cuatro categorías de datos:

a) Datos de carácter personal o datos personales: El artículo 2, letra f) de la Ley N°19.628 señala que los datos personales son "los relativos a cualquier información que se refiera a personas naturales, identificadas o identificables"[72], los datos personales comprenden todo tipo de datos que se refieran a una persona, independientemente de la naturaleza y forma de representación de dichos datos, ya sea sonido, imagen, entre otras, siendo este un concepto amplio.

Estos datos solo se refieren a persona natural o física, por lo tanto, no es dato personal aquél que se refiera a una persona jurídica, esta es la tendencia generalmente establecida por los Estados que regulan dicho derecho, ya que se entiende que la protección de los datos personales deriva de la dignidad humana. Por último, cabe analizar el alcance de la protección de datos personales que se refiere a personas identificadas o identificables, una persona identificada se refiere a aquella cuya identidad ya ha sido establecida de manera clara y precisa, por ejemplo, si se tienen los datos como el nombre completo, número de identificación (RUN), u otra información que permita identificar a una persona, se trata de una persona identificada, mientras que una persona identificable es aquella que no ha sido identificada de manera directa, pero su identidad puede ser determinada con información adicional que tiene posesión o que puede acceder la entidad que trata los datos, pudiendo llegar a identificar a una persona a través de la combinación de diferentes datos o algún otro método razonable.

b) Datos sensibles: El artículo 2 letra g) señala que son:

> "aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida o intimidad, tales como los hábitos personales, el origen racial, las tecnologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual."[73]

[71] CERDA, A. (2012). Legislación sobre protección de las personas frente al tratamiento de datos personales. Santiago, Centro de Estudios en Derecho Informático, Universidad de Chile. p. 16.
[72] Artículo 2, letra f) de la Ley 19.628.
[73] Artículo 2, letra g) de la Ley 19.628.

La definición legal de datos sensibles es amplia, lo que implica que en cada caso específico será el juez quien determine si se trata de datos de esta naturaleza. Esto significa que la normativa sobre datos sensibles se aplica en situaciones de conflicto jurídico.

c)Dato estadístico: El artículo 2 letra e) señala que es el dato que, "en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable"[74].

d)Dato caduco: El artículo 2 letra d) señala que es aquel 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"[75].

Además, la ley establece otras categorías de datos:

a) Datos personales provenientes de fuentes de acceso público: Se establece en el artículo 4 inciso quinto de la ley, siendo una excepción a la regla general del consentimiento del titular, para el tratamiento de este tipo datos. Estos datos, se refieren a aquellos datos de fuentes accesibles al público del artículo 2 letra i) de la Ley.

b) Datos de carácter económico, bancario o comercial: Estos datos se establecen en el Título III de la Ley N°19.628, específicamente en los artículos del 17 al 19, se refieren a este tipo de datos. Según la doctrina, se considera este tipo de datos como aquellos relacionados con obligaciones o deudas, es decir, datos patrimoniales. Es importante destacar que esta categoría tiene un nivel de protección inferior, ya que constituye una excepción al requisito general del consentimiento del titular.

De acuerdo con esta clasificación, algunos tipos de datos tienen una protección mayor que otros. Los datos que no se consideran sensibles tienen una protección inferior, donde el consentimiento del titular es menos relevante en comparación con otros tipos de datos. Por otro lado, los datos sensibles están sujetos a restricciones, así se establece en el artículo 10, "no pueden ser objeto de tratamiento los datos sensibles, salvo cuando la ley lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares"[76]. En resumen, mientras que el tratamiento de datos personales está permitido en general, el tratamiento de datos sensibles tiene limitaciones específicas.

Es importante tener en cuenta que la calificación inicial de los datos la realiza el responsable del registro o banco de datos. Su interés suele ser contrario al del titular de los datos, ya que intentará evitar

[74] Artículo 2, letra e) de la Ley 19.628.
[75] Artículo 2, letra d) de la Ley 19.628.
[76] Artículo 10 de la Ley 19.628.

que se clasifiquen como sensibles para poder tratarlos sin las restricciones legales que conlleva su tratamiento.

La falta de una definición clara de datos de mera identificación y la amplia definición de datos sensibles generan la necesidad de establecer un régimen especial para ambos tipos de datos. En la práctica, se considera que todas las fuentes son accesibles al público, salvo aquellas que estén específicamente protegidas por leyes, normas administrativas o acuerdos de confidencialidad.

4.8 Derechos de los titulares de los datos personales

Las legislaciones de protección de datos, incluyendo la de Chile, han establecido cuatro derechos fundamentales para los titulares de datos personales. Los derechos que se establecen en la Ley N°19.628 son:

> "aquellos establecidos en el artículo 12 de esta Ley, y se denominan conjuntamente los "derechos ARCO". Recordemos que ARCO corresponde a la sigla de (A)cceso a la información de los datos personales del titular que tiene el responsable; (R)ectificación de datos erróneos o desactualizados; (C)ancelación de datos que puedan eliminarse al ser innecesario su tratamiento; y (O)posición del titular a que se efectúen ciertos tratamientos con estos datos; y que estos derechos pueden ser ejercidos por los titulares de datos personales frente al responsable del tratamiento de éstos."[77]

Según la ley en el artículo 13, estos derechos son irrenunciables y no pueden ser limitados por ningún acto o convención, ya que constituyen el núcleo del derecho fundamental a la protección de datos.

Los derechos establecidos en el título II de la Ley N°19.628 surgen como una contrapartida a la autorización legal para el tratamiento de datos personales. La ley permite el tratamiento de datos de terceros bajo ciertas condiciones, pero también otorga herramientas para garantizar la veracidad de los datos y el cumplimiento de requisitos legales. Si no se cumplen estas condiciones, la ley garantiza a los titulares los derechos ARCO.

Cabe mencionar que, la legitimación activa corresponde a las personas naturales que la ley llama titulares de datos, es quien tiene legitimidad para ejercer sus derechos, tales derechos se pueden ejercer tanto de forma personal por el titular como a través de representante legales o voluntarios, ya que si una

[77] NEHME, F. (s/f). Ejercicio de derechos ARCO y su tramitación. Recuperado el 15 de junio de 2023, de https://fn.cl/comunicaciones/ejercicio-de-derechos-arco-y-su-tramitacion

persona se encuentra en el extranjero o un menor de edad deberían poder ser representados legítimamente para ejercer sus derechos.

A) Derecho de acceso

El derecho primario en protección de datos establece que el responsable del tratamiento de datos debe proporcionar información específica sobre los datos personales que están siendo procesados. Esto incluye detalles sobre el origen de los datos, los propósitos del tratamiento y los destinatarios a quienes se comunican o se pretende comunicar dicha información.

Además, los responsables del tratamiento de datos tienen la obligación de proporcionar información comprensible a los interesados, utilizando un lenguaje claro y sencillo.

El derecho de acceso está establecido en el artículo 12, estableciendo que:

> "Toda persona tiene derecho a exigir a quien sea responsable de un banco, que se dedique en forma pública o privada al tratamiento de datos personales, información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente."[78]

Los interesados tienen el derecho de solicitar una copia gratuita de su registro, pero solo pueden ejercer este derecho después de al menos seis meses desde la última vez que lo solicitaron. Esta disposición busca equilibrar los intereses de quienes manejan datos, como las oficinas de crédito, evitando solicitudes constantes de documentación gratuita. El derecho de acceso se puede ejercer en cualquier momento, ya sea visualizando los datos en pantalla u obteniendo copias después del período de espera.

Este derecho se hace exigible mediante,

> "la obligación a los organismos públicos de registrar las bases de datos en un registro público, a cargo del Registro Civil e Identificación. Este registro público debe contener información acerca del fundamento jurídico de su existencia, su finalidad, tipos de datos almacenados y descripción del universo de personas que comprende. Lamentablemente esta obligación no se ha hecho extensible a las entidades privadas, quedando estas últimas exentas de

[78] Artículo 12, inciso primero de la Ley 19.628.

la obligación de registrar sus bases de datos, y mermando con ello la capacidad de las personas naturales de ejercer su derecho de información y acceso."[79]

B) Derecho de rectificación

El derecho de rectificación permite al titular de los datos solicitar a la persona responsable la modificación de los datos personales "cuando estos sean erróneos, inexactos, equívocos o incompletos"[80]. Este derecho se deriva del principio de calidad, que exige que quienes manejan datos personales los mantengan completos y actualizados según sea necesario para cumplir con los fines previstos.

El artículo 2 letra j) de la Ley N°19.628 define la modificación o rectificación como "todo cambio en el contenido de los datos almacenados en registros o bancos de datos"[81]. Su objetivo es corregir o complementar aquellos datos que se encuentren inexactos o incompletos en la base de datos. Además de otras regulaciones específicas que afectan este asunto, es importante destacar que el ejercicio del derecho de rectificación es gratuito y el responsable del tratamiento de datos tiene la obligación de comunicar cualquier rectificación a todas las personas a las que se les hayan proporcionado dichos datos.

En virtud de esta ley, el titular de los datos tiene el derecho de solicitar la modificación de sus datos personales, y el responsable del banco de datos tiene la obligación correspondiente de llevar a cabo dicha modificación, siempre y cuando se demuestre que los datos son incorrectos, inexactos, equívocos o incompletos, tal como se establece en el artículo 12 inciso segundo.

C) Derecho de cancelación o eliminación

El artículo 2 letra h) conceptualiza la eliminación o cancelación como "la destrucción de datos almacenados en registros o bancos de datos, cualquiera fuere el procedimiento empleado para ello"[82].

Además, el artículo 12 inciso tercero, establece que el titular, "sin perjuicio de las excepciones legales, podrá, además, exigir que se eliminen, en caso de que su almacenamiento carezca de fundamento legal o cuando estuvieren caducos"[83], teniendo que ser eliminados de la base de datos. El tratamiento de datos pierde su base legal cuando se realiza en violación de lo establecido por la ley o, por ejemplo, si la ley que lo autorizaba es derogada.

[79] VIOLLIER, P. (2018). El Estado de la protección de datos personales en Chile. Derechos Digitales. p. 25.
[80] CONSEJO PARA LA TRANSPARENCIA. (s/f). Formulario derecho ARCO. Recuperado el 17 de junio de 2023, de https://derechosarco.cplt.cl/Paginas/Inicio.aspx
[81] Artículo 2, letra j) de la Ley 19.628.
[82] Artículo 2, letra h) de la Ley 19.628.
[83] Artículo 12, inciso tercero de la Ley 19.628.

El derecho de cancelación permite solicitar la eliminación de datos personales que sean innecesarios, excesivos o que se estén utilizando sin el consentimiento del interesado o sin una base legal que lo justifique. Sin embargo, la cancelación no aplica cuando exista una obligación legal o contractual de conservar los datos.

Por ejemplo, si una persona proporciona sus datos personales a una empresa para obtener un crédito, no puede luego ejercer el derecho de cancelación mientras la relación contractual esté vigente.

Al igual que con el derecho de rectificación, el responsable del tratamiento de datos no puede exigir ninguna compensación cuando el titular ejerce este derecho. Además, el responsable debe eliminar los datos de forma voluntaria tan pronto como detecte que su almacenamiento no tiene base legal o cuando hayan caducado en relación con su finalidad, ya que de lo contrario podría incurrir en responsabilidad.

D) Derecho de oposición

El derecho de oposición es el último de los derechos ARCO y permite al titular de los datos oponerse al tratamiento de sus datos personales por una razón legítima basada en que el tratamiento ha iniciado sin su consentimiento, salvo excepciones legales. Por ejemplo, el titular puede ejercer este derecho, "si en caso estén usando sus datos personales para otros motivos, podrá generar una solicitud para restringir su uso"[84].

El derecho de oposición está establecido en el artículo 3, inciso segundo, aunque de manera ambigua: "El titular puede oponerse a la utilización de sus datos personales con fines de publicidad, investigación de mercado o encuestas de opinión"[85].

Además, la Ley 20.285 sobre acceso a la información pública establece en su artículo 20 que los organismos públicos deben comunicar a terceros cuando se solicita información que puede afectar sus derechos, permitiéndoles ejercer su facultad de oponerse a la entrega de los documentos, especialmente cuando contienen datos personales.

[84] TECNOWEB. (s/f). Ley de Datos Personales ARCO. Recuperado el 19 de junio de 2023, de https://www.tecnoweb.net/es-cl/ley-arco
[85] Artículo 3, inciso segundo de la Ley 19.628.

4.8.1 Otros derechos de los titulares

Además de los derechos de acceso, rectificación, cancelación y oposición, que son los cuatro derechos principales establecidos en la legislación chilena, denominados derechos ARCO, también cabe mencionar otros derechos contenidos en la Ley N°19.628.

A) Derecho de bloqueo

La ley de protección de datos también contempla el derecho bloqueo de datos, que deriva del ejercicio del derecho de oposición, establecido en el artículo 2 letra b), el cual consiste en "la suspensión temporal de cualquier operación de tratamiento de datos almacenados"[86], operando respecto de los datos personales cuando su exactitud no puede ser establecida o su vigencia es cuestionable, y de los cuales no corresponde su cancelación.

En la práctica, el bloqueo de datos implica la prohibición de compartir la información bloqueada con terceros. Además, se puede solicitar la cancelación o bloqueo de los datos en listas utilizadas para comunicaciones comerciales, ejerciendo el derecho de no querer aparecer en dichos registros, ya sea temporal o permanentemente, y cada vez que los datos se hayan proporcionado de forma voluntaria.

B) Obligación de comunicación a terceros

Dicha obligación está establecida en el artículo 12 inciso final, existe como contrapartida al derecho al acceso, y establece que:

> "Si los datos personales cancelados o modificados hubieren sido comunicados previamente a personas determinadas o determinables, el responsable del banco de datos deberá avisarles a la brevedad posible la operación efectuada. Si no fuese posible determinar las personas a quienes se les hayan comunicado, pondrá un aviso que pueda ser de general conocimiento para quienes usen la información del banco de datos."[87]

C) Derecho de copia

Cuando el titular solicita:

> "la información, modificación o eliminación de los datos serán absolutamente gratuitas, debiendo proporcionarse, además, a solicitud del titular, copia del registro alterado en la parte pertinente. Si se efectuasen nuevas modificaciones o eliminaciones de datos, el titular podrá, asimismo, obtener sin costo copia del registro actualizado, siempre que haya transcurrido a lo

[86] Artículo 2, letra b) de la Ley 19.628.
[87] Artículo 12, inciso final de la Ley 19.628.

menos seis meses desde la precedente oportunidad en que hizo uso de este derecho. El derecho a obtener copia gratuita sólo podrá ejercerse personalmente."[88]

D) Gratuidad en el ejercicio de los derechos

Según la ley, el uso de estos derechos es gratuito, lo que significa que el responsable del banco de datos debe asumir cualquier costo asociado a su cumplimiento. El artículo 12 inciso quinto establece claramente que la modificación, eliminación o información de los datos serán gratuitos absolutamente.

Sin embargo,

> "se omite mencionar el bloqueo, de lo que se colige que el ejercicio de este derecho de bloqueo puede estar sujeto a cobro, que en todo caso, nunca podrá ser de tal entidad que imposibilite su ejercicio, es decir, debe ser un cobro racional y proporcional."[89]

En cuanto al derecho de copia, la gratuidad está sujeta a que transcurra un mínimo de seis meses entre cada ejercicio de este derecho.

E) Irrenunciabilidad

La Ley N°19.628 establece derechos que son considerados de orden público, debido a su vínculo con la garantía constitucional del respeto a la vida privada. Esto se refleja en el artículo 13, que enfatiza que los titulares tienen el derecho a bloqueo, cancelación, modificación o información de sus datos personales, sin que estos derechos puedan ser limitados por ninguna convención o acto.

En consecuencia, "se prohíbe la exclusión o limitación del ejercicio de estos derechos. Cualquier pacto en contrario adolecerá de nulidad absoluta, conforme a los artículos 10 y 1466 del Código Civil"[90].

4.8.2 Límites al ejercicio de los derechos de los titulares

El artículo 13 de la ley de protección de datos personales establece que, los titulares tienen el derecho a bloqueo, cancelación, modificación o información de sus datos personales, sin que estos derechos puedan ser limitados por ninguna convención o acto.

Sin embargo, la ley establece en el artículo 15 la posibilidad de limitar el ejercicio de estos derechos en las siguientes hipótesis:

[88] Artículo 12, inciso quinto de la Ley 19.628.
[89] ORTIZ, P. J. (2003). Derechos del titular de datos y habeas data en la Ley 19.628. Revista chilena de derecho informático, (2). p. 21.
[90] SILVA, J. W. (2001). Tratamiento de datos personales y protección de la vida privada. Universidad de los Andes. p. 49.

a) Cuando obstaculice las funciones de supervisión de un organismo público, como en el caso de solicitar datos tributarios actuales al Servicio de Impuestos Internos.

b) Cuando infrinja el derecho de reserva o secreto establecido por leyes o regulaciones, como en el caso de datos personales en expedientes judiciales confidenciales.

c) Cuando afecte la seguridad nacional o el interés público. La determinación de esta situación dependerá de la evaluación del juez, considerando los hechos específicos relacionados con la solicitud de datos por parte del titular.

d) Datos almacenados según mandato legal, a menos que la ley lo permita.

4.9 Utilización o tratamiento de los datos personales

El principio del libre tratamiento de datos personales se establece de manera amplia, pero la ley establece que dicho tratamiento solo puede llevarse a cabo con la autorización del titular de los datos o de acuerdo con lo que estable el artículo 4 de la Ley: "El tratamiento de los datos personales sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello"[91].

Primero, si el titular de los datos personales autoriza el tratamiento de estos, dicha autorización está sujeta a las siguientes reglas:

A) La autorización para el tratamiento de datos personales debe ser por escrito e informada. Se debe proporcionar al titular de los datos información clara sobre la finalidad del tratamiento y la posible comunicación de sus datos al público, para que pueda decidir el nivel de divulgación que está dispuesto a permitir.

B) La autorización para el tratamiento de datos personales puede ser revocada por escrito, pero dicha revocación no tiene efecto retroactivo.

Una segunda posibilidad, es que el tratamiento de datos personales puede ser autorizado por la ley, ya sea a través de una ley especial o mediante disposiciones generales establecidas en la Ley N°19.628.

Esta ley, en su artículo 4 autoriza el tratamiento de datos personales sin el consentimiento del titular en cuatro casos específicos:

[91] Artículo 4, inciso primero de la Ley 19.628.

a) En el caso de tratamiento de datos personales que provengan o que se recolecten de fuentes accesibles al público, el artículo 4 inciso quinto establece esto siempre cuando se trate de:

1) de datos personales de carácter económico, financiero, bancario o comercial, 2) de datos personales que se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento, o 3) de datos personales que sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes y servicios.

b) Las personas jurídicas privadas pueden llevar a cabo el tratamiento de datos personales bajo ciertas condiciones específicas establecidas en el artículo 4 inciso final:

> "Tampoco requerirá de esta autorización el tratamiento de datos personales que realicen personas jurídicas privadas para el uso exclusivo suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquéllos."[92]

c) El artículo 20 establece que "el tratamiento de datos personales por parte de un organismo público sólo podrá efectuarse respecto de las materias de su competencia y con sujeción a las reglas precedentes. En esas condiciones, no necesitará el consentimiento del titular"[93].

d) Cuando el tratamiento de datos personales se efectúe para el otorgamiento o determinación de beneficios de salud para sus titulares, o salvo que la ley lo autorice, situaciones establecidas en el artículo 10. Entonces, en situaciones excepcionales como las ya descritas, los responsables de registros o bancos de datos pueden tratar datos sensibles de una persona, sin el consentimiento de sus titulares.

4.9.1 Utilización de datos personales en obligaciones de carácter económico, financiero, bancario o comercial

El inciso tercero del artículo 9 de la ley establece la prohibición de realizar predicciones o evaluaciones de riesgo comercial que no se basen únicamente en información objetiva sobre protestos o morosidades de personas naturales o jurídicas. Esta disposición enfatiza la importancia de utilizar fuentes de información financiera confiables respaldadas por parámetros objetivos. En caso de infringir esta prohibición, el responsable de la base de datos debe eliminar inmediatamente la información y el titular puede ser sujeto a indemnización por los perjuicios ocasionados.

[92] Artículo 4, inciso final de la Ley 19.628.
[93] Artículo 20 de la Ley 19.628.

Uno de los aspectos más controvertidos de la Ley N°19.628 se refiere a los datos financieros, ya que según el artículo 4, no se necesita el consentimiento del titular para el tratamiento y transferencia de datos económicos, financieros, bancarios o comerciales. Esta disposición plantea preocupaciones significativas en cuanto a los derechos individuales y puede ser perjudicial en algunos casos.

El título III de la Ley N°19.628 aborda la protección de la información relacionada con obligaciones económicas, financieras, bancarias o comerciales. El artículo 17 establece:

> "el marco por el cual los responsables de los registros y bancos de datos sólo podrán comunicar información que verse sobre obligaciones de carácter económico, financiero, bancario o comercial, en determinadas circunstancias contempladas por ley (que consten en pagares, letras de cambio protestados, cheques también protestados, entre otros). Es relevante mencionar además que el segundo inciso de la norma en análisis establece que también podrán comunicarse aquellas otras obligaciones de dinero que determine el Presidente de la República mediante Decreto Supremo, las que deberán estar sustentadas en instrumentos de pago o de crédito válidamente emitidos, en los cuales conste el consentimiento expreso del deudor u obligado al pago y su fecha de vencimiento. Como se puede ver, la norma establece determinadas causales expresas respecto de la cual entidades que administran la información financiera de los particulares pueden ser comunicadas a otras personas"[94].

Según el artículo 18 de la ley, existen restricciones claras en la comunicación de datos relacionados con una persona identificada o identificable en dos situaciones. Primero, después de transcurridos cinco años desde que la obligación correspondiente se volvió exigible, no se podrán comunicar dichos datos. Segundo, una vez que la obligación ha sido pagada o legalmente extinguida, no se puede continuar compartiendo información sobre esa obligación. Sin embargo, es importante destacar que la información relevante puede ser comunicada a los tribunales en el contexto de juicios pendientes. Estos artículos establecen los límites generales para la manipulación de la información financiera por parte de entidades que gestionan registros de datos.

Por último, el artículo 19 en términos generales establece que el pago o extinción de las obligaciones no afecta la vigencia de los datos correspondientes según el artículo 12, siempre y cuando se cumplan los plazos establecidos. En caso de que el pago o extinción sea realizado directamente por el acreedor, este deberá informar al responsable del registro o banco de datos accesible al público que

[94] ZEGERS, I. (2021). La finalidad como estándar de protección de datos personales de carácter económico, financiero, bancario y comercial: un análisis desde la evolución normativa nacional y la regulación supranacional. [Tesis de licenciatura, Universidad de Chile]. p. 15-16. https://repositorio.uchile.cl/bitstream/handle/2250/184367/La-finalidad-como-estandar-de-proteccion-de-datos-personales-de-caracter-economico.pdf?sequence=1&isAllowed=y

comunicó previamente la morosidad o protesto. El deudor puede optar por solicitar directamente la modificación de los datos y liberar al acreedor de esa responsabilidad, siempre y cuando proporcione pruebas de pago por escrito. Aquellos que manejen datos de fuentes accesibles al público deben modificar o bloquear los datos una vez que se comunique el pago o extinción de la obligación, dentro de un plazo de tres días. El incumplimiento de aquellas obligaciones será sancionado según lo establecido en el artículo 16.

4.9.2 Tratamiento de datos por los organismos públicos

Los organismos públicos suelen tratar regularmente datos personales para diversos propósitos, como "identificar a los ciudadanos, recaudar impuestos, establecer políticas públicas"[95]. La Ley N°19.628 establece reglas específicas aplicables al tratamiento de datos por parte de los organismos públicos.

El título IV de la ley aborda el tratamiento de datos personales por parte de organismos públicos y establece ciertas condiciones y prerrogativas. Según el artículo 20, los organismos públicos solo pueden tratar datos personales relacionados con sus competencias y de acuerdo con las normas de la ley. En estas circunstancias, no se requiere el consentimiento del titular de los datos. Esta disposición se suma a las del artículo 15, que constituyen un régimen excepcional a favor del Estado y sus organismos. En resumen, cuando un organismo público trata datos personales en relación con sus competencias y cumpliendo las normas legales, no se necesita el consentimiento del titular, y no se puede solicitar la modificación, cancelación o bloqueo de datos que obstaculicen sus funciones de supervisión. Además, se establece que no se puede ejercer el derecho de modificación, cancelación o bloqueo de datos almacenados. Por ejemplo, el Ministerio de Hacienda puede utilizar datos personales para la administración de los recursos del Estado, pero no puede hacerlo para funciones propias del Ministerio de Educación. Cuando un organismo público solicita datos personales a otro, debe indicar claramente la finalidad para la cual los solicita, y el segundo organismo tiene la obligación de verificar que dicha finalidad esté dentro de las funciones del primero. En caso contrario, la cesión de datos debe ser denegada.

El artículo 21 establece que "los organismos públicos que sometan a tratamiento datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias, no podrán comunicarlos una vez prescrita la acción penal o administrativa, o cumplida o prescrita la sanción o la

[95] ECIJA. (16 de noviembre de 2020). Tratamiento de datos personales por los organismos públicos en Chile. Recuperado el 20 de junio de 2023, de https://ecija.com/sala-de-prensa/tratamiento-de-datos-personales-por-los-organismos-publicos-en-chile/

pena"[96]. Esta disposición garantiza el derecho al olvido, que busca facilitar la reinserción social de las personas que han sido afectadas por estas anotaciones, especialmente en el ámbito laboral. Por otra parte, el inciso segundo, establece que quedan excluidos los casos en los que los tribunales de justicia u otros organismos públicos, dentro de su competencia, soliciten dicha información. En tales situaciones, se les exige mantener confidencialidad y reserva de esta, y se les aplicarán las disposiciones establecidas en los artículos 5, 7, 11 y 18 de la ley. Por ejemplo, si un organismo estatal guarda información sobre sanciones o infracciones cometidas por un ciudadano, pero estas fueron cumplidas, no podrá compartirlas, a menos que sean solicitadas por los tribunales de justicia u otros organismos públicos que respeten la reserva de dichos datos.

Por último, el artículo 22 establece que el Servicio de Registro Civil e Identificación mantendrá un registro público de los bancos de datos personales administrados por organismos públicos. En este registro se incluirá la base legal de su existencia, su finalidad, los tipos de datos almacenados y una descripción del grupo de personas involucradas. Estos detalles serán establecidos en un reglamento. El organismo público responsable del banco de datos deberá proporcionar esta información al Servicio de Registro Civil e Identificación al iniciar sus operaciones y comunicar cualquier cambio en los factores mencionados en un plazo de quince días.

En consecuencia, cualquier banco de datos establecido por un organismo estatal debe ser registrado en el Servicio de Registro Civil. Este registro incluirá información sobre su existencia, propósito, tipos de datos almacenados y descripción del grupo de personas involucradas. Además, este registro será de acceso público.

Además de las obligaciones específicas establecidas en los artículos 20, 21 y 22, la Ley N°19.628 impone a los organismos públicos del Estado el cumplimiento de todas las demás normas aplicables a los responsables de tratamiento de datos. Esto incluye disposiciones relevantes contenidas en los artículos 7 y 11 de la Ley N°19.628. El Estado tiene la misma responsabilidad de proteger los datos personales que cualquier otro responsable o encargado. Sin embargo, en el caso del Estado, esta responsabilidad se ve reforzada por la obligación de probidad administrativa de los servidores públicos establecida en la Ley 20.880.

4.10 De la responsabilidad por las infracciones a esta ley

El artículo 23 establece que el responsable de un banco de datos personales ya sea una persona natural, persona jurídica privada u organismo público, será responsable de indemnizar tanto el daño

[96] Artículo 21, inciso segundo de la Ley 19.628.

patrimonial como el daño moral ocasionado por el tratamiento inapropiado de los datos. Además, deberá tomar las medidas necesarias para eliminar, modificar o bloquear los datos de acuerdo con las solicitudes del titular o las órdenes judiciales.

La acción correspondiente puede presentarse junto con la reclamación para determinar la infracción, sin perjuicio de lo establecido en el artículo 173 del Código de Procedimiento Civil. En caso de infracciones no contempladas en los artículos 16 y 19, incluyendo la indemnización de perjuicios, se aplicará el procedimiento sumario. El juez tomará todas las medidas necesarias para garantizar la protección de los derechos establecidos por esta ley. La apreciación de la prueba se realizará en conciencia por el juez.

El monto de la indemnización será determinado prudencialmente por el juez, teniendo en cuenta las circunstancias del caso y la gravedad de los hechos.

Cabe señalar que, la Ley N°19.628 regula:

> "un supuesto de responsabilidad extracontractual aún cuando podría parecer que, en los casos en que el titular otorgue expresamente y por escrito la autorización para el tratamiento de sus datos, se pueda dar lugar a un vínculo contractual. Esto resulta erróneo, toda vez que la autorización para tratar datos personales es un acto unilateral y no necesariamente un acuerdo de voluntades del que emanarán derechos y obligaciones. Por lo demás, nuestra doctrina es conteste al analizar el régimen de responsabilidad civil de la LPD, entendiendo que nos encontramos ante una regulación de orden extracontractual."[97]

4.11 Título Final

El artículo 24 de la ley incorpora dos nuevos incisos, el inciso segundo y tercero al artículo 127 del Código Sanitario, con el objetivo de garantizar una protección especial para los datos sensibles en el ámbito de la salud, como los contenidos en recetas médicas y resultados de análisis de laboratorios clínicos. Los nuevos incisos son los siguientes que se describen a continuación:

El artículo 24 inciso segundo establece que:

> "Las recetas médicas y análisis o exámenes de laboratorios clínicos y servicios relacionados con la salud son reservados. Sólo podrá revelarse su contenido o darse copia de

[97] PEÑA, S. A. (2019). Régimen de indemnización de perjuicios de la Ley N° 19.628 y la seguridad de datos personales. Análisis crítico del principio de seguridad de datos del artículo 11° de la Ley de protección a la vida privada y su aplicación práctica. [Tesis de licenciatura, Universidad de Chile]. p. 31. https://repositorio.uchile.cl/bitstream/handle/2250/175622/Regimen-de-indemnizacion-de-perjuicios-de-Ley-no-19628-y-la-seguridad-de-datos-personales.pdf?sequence=1

ellos con el consentimiento expreso del paciente, otorgado por escrito. Quien divulgare su contenido indebidamente, o infringiere las disposiciones del inciso siguiente, será castigado en la forma y con las sanciones establecidas en el Libro Décimo."[98]

Finalmente, el inciso final del artículo 24 señala que:

"Lo dispuesto en este artículo no obsta para que las farmacias puedan dar a conocer, para fines estadísticos, las ventas de productos farmacéuticos de cualquier naturaleza, incluyendo la denominación y cantidad de ellos. En ningún caso la información que proporcionen las farmacias consignará el nombre de los pacientes destinatarios de las recetas, ni el de los médicos que las expidieron, ni datos que sirvan para identificarlos."[99]

4.12 Mecanismos de protección

Una crítica importante hacia la Ley N°19.628 se debe a que:

"omitió establecer un adecuado sistema de control, a fin de cerciorarse del cumplimiento de sus preceptos; muy en especial, la ley prescinde de una autoridad de control que vele por la realización de sus mandatos, lo cual socava toda pretensión de obtener un mayor nivel de protección adecuado a los derechos de las personas concernidas."[100]

Esta deficiencia implica que las personas afectadas deben acudir a los tribunales ordinarios de justicia, ya sea mediante acciones constitucionales de protección o utilizando los mecanismos establecidos en la ley, para hacer valer sus derechos y protegerse del uso indebido de sus datos por parte de terceros. Los costos asociados a los procesos judiciales y el desconocimiento generalizado sobre cómo se tratan sus datos personales dificultan aún más la aplicación de la Ley N°19.628.

La Ley 20.285 sobre Acceso a la Información Pública, en su artículo 31 crea al Consejo para la Transparencia, estableció a su vez en el artículo 33 letra m), "velar por el adecuado cumplimiento de la ley N°19.628, de protección de datos de carácter personal, por parte de los órganos de la Administración del Estado"[101]. Sin embargo, dicho Consejo carece de la facultad de imponer sanciones por incumplimiento de estas obligaciones. Como resultado, el incumplimiento de la ley por parte de los

[98] Artículo 24, inciso segundo de la Ley 19.628.
[99] Artículo 24, inciso final de la Ley 19.628.
[100] CERDA, A. (2003). La autoridad de control en la legislación sobre protección frente al tratamiento de datos personales. [Tesis de Magíster, Universidad de Chile]. p. 5. https://repositorio.uchile.cl/bitstream/handle/2250/106762/cerda_a.pdf?sequence=3&isAllowed=y
[101] Ley N° 20.285, Sobre acceso a la información pública. (11 de agosto de 2008). Artículo 33, letra m). Diario Oficial de la República de Chile, Santiago.

organismos públicos no ha disminuido. Además, en el caso de los organismos privados, el Consejo carece de atribuciones para hacer cumplir las disposiciones de la Ley N°19.628.

Los mecanismos de protección a los derechos de datos personales más importantes son el recurso de protección y la acción de habeas data.

Tanto el recurso de protección como la acción de habeas data pueden aplicarse juntos en una situación específica. Primero, el recurso de protección se utiliza para restaurar de inmediato el imperio del derecho cuando el responsable del tratamiento de datos comete una acción u omisión arbitraria o ilegal que vulnera derechos de los titulares de los datos. Después, de obtenida una sentencia producto del recurso de protección, se puede utilizar la acción de habeas data para pedir la indemnización por los perjuicios ocasionados ante el tribunal respectivo.

4.12.1. El recurso de protección

En caso de ser víctimas de un tratamiento ilegítimo de sus datos personales, las personas tienen la opción de recurrir a la Corte de Apelaciones de su domicilio y presentar un recurso de protección, el cual se encuentra regulado por el:

> "artículo 20 de la Constitución Política y el Autoacordado de la Corte Suprema de 1.992. La parte final del artículo 20 señala que este recurso podrá interponerse sin perjuicio de los demás derechos que el afectado pueda hacer valer ante la autoridad o los tribunales correspondientes. Me parece que claramente la norma permite la interposición del recurso constitucional y la acción de habeas data."[102]

Este recurso se caracteriza por su informalidad, su carácter inquisitorio, la unilateralidad, rápido, concentrado, y de bajo costo para el recurrente. A través de este recurso, como se establece en el artículo 20, cualquier individuo puede solicitar a la Corte que tome medidas para poner fin a actos u omisiones arbitrarios o ilegales sufra privación, perturbación o amenaza que afecten algunos de sus derechos fundamentales del artículo 19, como en este caso es el derecho a la protección de los datos personales del titular establecido en el artículo 19N°4 de la Constitución, ante lo cual la Corte de Apelaciones, "adoptará de inmediato las providencias que juzgue necesarias para restablecer el imperio del afectado, sin perjuicio de los demás derechos que pueda hacer valer ante la autoridad o los tribunales correspondientes"[103].

[102] NAVARRETE, S. (2008). La protección de datos personales en Chile y la Ley 19.628. [Tesis de licenciatura, Universidad Austral de Chile]. p. 72. http://cybertesis.uach.cl/tesis/uach/2008/fjn321p/doc/fjn321p.pdf
[103] CONSTITUCIÓN POLÍTICA DE LA REPÚBLICA DE CHILE. [C.P.], art. 20. 17 de septiembre de 2005 (Chile).

Cabe señalar que, el artículo 12 de la Ley N°19.628 establece los derechos ARCO para sus titulares, pero puede suceder que por una acción u omisión arbitraria o ilegal del responsable del tratamiento de datos se vulneren derechos de los titulares distintos a los derechos ARCO, por ende, quedaría fuera del ámbito de aplicación del habeas data, por ello, ante este caso, se puede proceder con un recurso de protección con el objetivo de restablecer el imperio del derecho.

4.12.2 La acción de habeas data

En Chile, al igual que en muchas legislaciones, existe la posibilidad de que las personas afectadas recurran a los tribunales para proteger sus derechos en relación con el tratamiento de sus datos personales. Para ello, se puede optar por el procedimiento especial conocido como "acción de habeas data" establecido en la Ley N°19.628, principal mecanismo para otorgar protección expedita al que se ve afectado por el tratamiento de datos personales. Esta acción, deriva del Habeas Corpus o recurso de amparo.

La ley garantiza a las personas el derecho de solicitar a través del procedimiento de habeas data, "requerir datos personales suyos alojados en bases de datos, ya sean públicas o privadas"[104]. Esto les permite verificar la exactitud y veracidad de dichos datos.

El Habeas Data es una acción judicial autónoma y específica, con un objeto claramente definido y un proceso de tramitación concentrado. Además, no se limita a ser una acción cautelar, ya que la sentencia resultante tiene efectos de cosa juzgada. Asimismo, la sentencia puede incluir sanciones en caso de incumplimiento. La acción tiene un carácter preventivo, permitiendo al titular conocer la existencia de registros o bancos de datos que contengan información suya y acceder a ella. Además, tiene un carácter correctivo, ya que permite exigir la corrección, rectificación, cancelación o bloqueo de datos personales cuando su tratamiento es indebido e ilegal.

El bien jurídico protegido es la protección de los datos personales de los titulares, además de otros derechos, tales como, la autodeterminación informativa, el derecho a la protección de la vida privada o privacidad y la honra de la persona, la igualdad ante la ley, la protección de la dignidad humana, la libertad, también la legitimidad de la información.

El objeto de la acción de habeas data, tal como lo señala el inciso primero del artículo 16, se refiere a la protección de los derechos establecidos en el artículo 15, menciona los derechos de

[104] PODER JUDICIAL TV. (s/f). Reportaje Judicial: El recurso de habeas data y su aplicación en Chile. Recuperado el 23 de junio de 2023, de https://www.poderjudicialtv.cl/programas/reportaje/reportaje-judicial-el-recurso-de-habeas-data-y-su-aplicacion-en-chile/

información, modificación, bloqueo y cancelación, que pueden ser objeto de la acción de habeas data, es decir, el habeas data "faculta a los titulares a solicitar judicialmente la exhibición de sus datos personales almacenados en un registro o banco, o requerir su rectificación, eliminación, complementación o reserva"[105].

Sin embargo, los derechos de copia y oposición no son mencionados en el artículo 15, lo cual no parece justificado para excluirlos de esta protección específica. Aunque el derecho de copia puede entenderse implícito en el derecho de modificación o cancelación establecido en el artículo 15.

Este enfoque interpretativo no puede aplicarse al derecho de oposición establecido en el inciso segundo del artículo 3, por lo que parece quedar fuera del ámbito de protección de esta acción. No obstante, esto no impide que el derecho de oposición pueda ejercerse a través de una acción ordinaria de responsabilidad civil o un recurso de protección.

Además de amparar los derechos mencionados, la acción de habeas data también tiene por objeto, la indemnización de los perjuicios causados, y establecer una responsabilidad infraccional que puede dar lugar a sanciones administrativas.

El tribunal competente para conocer de esta acción según lo establecido en el artículo 16 es el "juez de letras en lo civil del domicilio del responsable"[106], es decir, el domicilio del demandado. Esta competencia se rige por la regla general establecida en el artículo 134 del Código Orgánico de Tribunales. El procedimiento es breve y sumario.

El legitimado activo para interponer la acción de acuerdo con el inciso primero del artículo 16 solo puede ser el titular de los datos que se ha visto vulnerado en los derechos reconocidos por la Ley N°19.628 y bajo ciertas causales, puede ser solamente una persona natural, chilena o extranjera.

Por otra parte, el legitimado pasivo:

> "es el responsable del banco de datos, sea particular o público. Asimismo, la ley establece, en su artículo 14, una regla especial, la que determina que en el evento en que los datos personales se encuentren en una base de datos a la cual tienen acceso diversos organismos, el titular de los datos puede demandar la información a cualquier de ellos, en cuyo caso, los sujetos pasivos pueden ser dos o más organismos privados o públicos."[107]

[105] WILKINS, J (2014). Régimen legal nacional de protección de datos personales. Biblioteca del Congreso Nacional de Chile. p. 4.
[106] Artículo 16, inciso primero de la Ley 19.628.
[107] NOGUEIRA, H. (2005). Autodeterminación informativa y hábeas data en Chile e información comparativa. Anuario de derecho Constitucional latinoamericano, 2(11). p. 466.

Cabe mencionar, si es una persona jurídica, se debe demandar a quienes tengan su representación judicial, además si se trata de un organismo público sin personalidad jurídica propia, se debe demandar al Consejo de Defensa del Estado.

El procedimiento judicial establecido en el artículo 16 de la ley se divide en dos tipos, un procedimiento ordinario o un procedimiento especial, dependiendo de la causa que origine la acción.

A) Procedimiento ordinario del Habeas Data

El procedimiento ordinario se aplica en las siguientes causales. La primera causal, de acuerdo con el artículo 16, se aplica si el responsable del registro o banco de datos no se pronuncia sobre la solicitud del requirente (titular de los datos) dentro de dos días hábiles. También se aplica, si el responsable del registro o banco de datos deniega por una causa distinta de la seguridad de la Nación o el interés nacional. La segunda causal, se aplica cuando se vulneran los artículos 17 y 18 de la Ley N°19.628.

Tal como lo establece el artículo 16 de la Ley N°19.628 el procedimiento se sujetará a las siguientes reglas:

> "La reclamación debe señalar la infracción cometida y los hechos que la configuran. Entendemos que para la ley el no respeto de los derechos por ella concedidos es suficiente para hablar de infracción a sus normas. Aunque la ley no lo diga expresamente, se deduce que la reclamación ha de ser escrita."[108]

Asimismo, el artículo 16, letra a) dispone que: "La reclamación señalará claramente la infracción cometida y los hechos que la configuran, y deberá acompañarse de los medios de prueba que los acrediten, en su caso"[109]. El significado de "en su caso" puede interpretarse de que este requisito no siempre es necesario, ya que la posibilidad de acompañar medios de prueba dependerá de la naturaleza infracción.

El tribunal de acuerdo con el artículo 16 letra b) ordenará la notificación de la reclamación por cédula, la cual será dejada en el domicilio del responsable del banco de datos correspondiente. De igual manera, la sentencia que se dicte también será notificada de la misma forma.

El responsable del banco de datos de acuerdo con el artículo 16 letra c):

[108] SILVA, J. W. (2001). Tratamiento de datos personales y protección de la vida privada. Universidad de los Andes. p. 52.
[109] Artículo 16, letra a) de la Ley 19.628.

"deberá presentar sus descargos dentro de quinto día hábil y adjuntar los medios de prueba que acrediten los hechos en que los funda. De no disponer de ellos, expresará esta circunstancia y el tribunal fijará una audiencia, para dentro de quinto día hábil, a fin de recibir la prueba ofrecida y no acompañada."[110]

La prueba rendida por las partes se aprecia en conciencia por el tribunal.

La sentencia definitiva, de acuerdo con el artículo 16 letra d) será dictada dentro de los tres días siguientes al vencimiento del plazo para presentar los descargos mencionado en el artículo 16 letra c), independientemente de si se presentaron o no descargos. En caso del que el tribunal haya decretado una audiencia de prueba, este plazo correrá una vez vencido el plazo fijado para ésta.

La sentencia definitiva debe notificarse por cédula, ya que según se establece en el artículo 16 letra e), "todas las resoluciones, con excepción de la indicada en la letra f) de este inciso, se dictarán en única instancia y se notificarán por el estado diario"[111]. Tal como se establece la excepción de la letra f) es la sentencia definitiva.

La sentencia definitiva de acuerdo con el artículo 16 letra f):

"será apelable en ambos efectos. El recurso deberá interponerse en el término fatal de cinco días, contado desde la notificación de la parte que lo entabla, deberá contener los fundamentos de hecho y de derecho en que se apoya y las peticiones concretas que se formulan."[112]

Una vez presentada la apelación, de acuerdo con el artículo 16 letra g), "el tribunal elevará de inmediato los autos a la Corte de Apelaciones respectiva. Recibidos los autos en la Secretaría de la Corte, el Presidente ordenará dar cuenta preferente del recurso, sin esperar la comparecencia de ninguna de las partes"[113].

En caso de que la Corte considere apropiado o se presente una solicitud fundamentada, puede disponer que los autos se traigan en relación y se lleven a cabo alegatos por parte de los abogados de las partes, en tal caso, la causa se añadirá de manera extraordinaria a la tabla correspondiente de la Sala.

[110] Artículo 16, letra c) de la Ley 19.628.
[111] Artículo 16, letra e) de la Ley 19.628.
[112] Artículo 16, letra f) de la Ley 19.628.
[113] Artículo 16, letra g) de la Ley 19.628.

El fallo que se pronuncie sobre la apelación, de acuerdo con el artículo 16 letra h), "no será susceptible de los recursos de casación"[114], sin embargo, procede el recurso de queja, de acuerdo con lo establecido en el artículo 545 del Código Orgánico de Tribunales.

B) Procedimiento especial del Habeas Data

El procedimiento especial se establece:

> "en los incisos tercero y cuarto del mismo artículo 16°, establece que, si la causal por la cual se negase el pleno ejercicio de los derechos de los titulares de datos fuese la seguridad de la nación o el interés nacional, el Habeas Data deberá ser deducido directamente ante la Corte Suprema. El sujeto pasivo de este procedimiento son solo los organismos públicos."[115]

La Corte Suprema solicitará informe de la autoridad de que se trate por la vía que considere más rápida, fijándole plazo al efecto, transcurrido el cual resolverá en cuenta la controversia. "De recibirse prueba, se consignará en un cuaderno separado y reservado, que conservará ese carácter aun después de afinada la causa si por sentencia ejecutoriada se denegare la solicitud del requirente."[116]

Los requisitos que debe contener la reclamación y la forma en que se debe notificar son los mismos que los establecidos en el procedimiento ordinario. La sala de la Corte Suprema que conozca la reclamación de acuerdo con el procedimiento especial, o la sala de la Corte de Apelaciones, que conozca la apelación, en el caso de un procedimiento ordinario, podrá, si lo considera apropiado o se le solicita con fundamento plausible, podrá traer los autos en relación para oír a los abogados de las partes, en tal caso, la causa se incluirá extraordinariamente a la tabla respectiva de la misma sala. En las reclamaciones basadas en la causal mencionada en el procedimiento especial, el presidente del tribunal dispondrá que la audiencia no sea pública.

C) Contenido y sanciones establecidas en la sentencia

Tal como lo establece el inciso quinto del artículo 16, en caso de acogerse la reclamación, la misma sentencia establecerá un plazo prudencial para que el registro o banco de datos dé cumplimiento con lo resuelto, podrá aplicar una multa de 1 a 10 UTM, como también determinar los perjuicios si le han sido solicitados, esto de acuerdo con los artículos 16, inciso quinto, y artículo 23 de la ley. Si se tratare de una infracción a lo establecido en los artículos 17 y 18, en relación con los datos personales de

[114] Artículo 16, letra h) de la Ley 19.628.
[115] Labbé Ibarra, S. A., y Latrille González, P. F. (2018). Protección de los datos personales en Chile, su tratamiento y comercialización. Análisis y críticas a la ley N° 19.628. [Tesis de licenciatura, Universidad Finis Terrae]. p. 36. https://repositorio.uft.cl/xmlui/bitstream/handle/20.500.12254/1494/LABBE-LATRILLE%202018.pdf?sequence=1&isAllowed=y
[116] Artículo 16, inciso tercero de la Ley 19.628.

carácter económico, financiero, bancario o comercial, la multa aplicable podrá ser de 10 a 50 UTM, esto último fue agregado en la Ley 19.812.

Por último, el inciso final del artículo 16 establece que:

> "La falta de entrega oportuna de la información o el retardo en efectuar la modificación, en la forma que decrete el Tribunal, serán castigados con multa de dos a cincuenta unidades tributarias mensuales y, si el responsable del banco de datos requerido fuere un organismo público, el tribunal podrá sancionar al jefe del Servicio con la suspensión de su cargo, por un lapso de cinco a quince días."[117]

D) Procedimiento residual

El procedimiento residual contemplado en el artículo 23 se aplica a las infracciones que no están contempladas en los artículos 16 y 19. Este procedimiento es de carácter sumario y procede cuando el responsable del registro o banco de datos no cumple con la obligación de avisar a terceros sobre la cancelación o corrección de datos, o el desarrollo de una base de datos por parte de un organismo público en áreas que no son de su competencia. En este procedimiento, el juez tiene la facultad de apreciar la prueba en conciencia.

E) Responsabilidad e indemnización de perjuicios

El inciso primero del artículo 23 de la ley señala que:

> "La persona natural o jurídica 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, sin perjuicio de proceder a eliminar, modificar o bloquear los datos de acuerdo a lo requerido por el titular o, en su caso, lo ordenado por el tribunal."[118]

En otras palabras, es posible obtener una indemnización por todos los perjuicios ocasionados debido al tratamiento indebido de los datos. Esto incluye la indemnización por los daños patrimoniales y también los daños morales. Es importante tener en cuenta que, al llevar a cabo la modificación o cancelación de los datos, ya se está realizando una forma de reparación de los daños. Sin embargo, si se busca obtener una indemnización adicional, será necesario demostrar estos perjuicios, incluyendo los de carácter moral. En este caso, el juez apreciará la prueba en conciencia. La naturaleza de esta responsabilidad se rige por las reglas del derecho común, es decir, el Código Civil, en concreto, las de

[117] Artículo 16, inciso final de la Ley 19.628.
[118] Artículo 23, inciso primero de la Ley 19.628.

responsabilidad extracontractual, ya que, en lo no previsto, se aplican las normas de los artículos 2314 y siguientes del código civil.

La acción de indemnización de perjuicios se puede reclamar a través de tres vías distintas:

> "La primera es a través del procedimiento previsto en el artículo 23 del cuerpo legal que posibilita interponer la acción indemnizatoria conjuntamente con la reclamación destinada a solucionar la infracción reclamada. El segundo procedimiento es mediante el juicio sumario referente a las infracciones no contempladas en los artículos 16 y 19, incluida la indemnización de perjuicios. El tercer procedimiento es mediante una acción de indemnización de perjuicios en un procedimiento ordinario, de acuerdo con las reglas generales."[119]

El inciso segundo del artículo 23 establece que el juez tomará todas las providencias que estime necesarias para garantizar la protección de los derechos establecidos por la Ley N°19.628, es decir, el tribunal puede adoptar todas las medidas cautelares que estime necesarias para la efectiva protección de los derechos que asegura esta ley. Por otra parte, pese a que la protección se establece en el presente artículo, se interpreta que de forma extensiva procede no solo en este caso, sino que, en todos los otros procedimientos, tanto en los procedimientos ordinario y especial del habeas data como el residual.

El inciso final del artículo 23 establece que: "El monto de la indemnización será establecido prudencialmente por el juez, considerando las circunstancias del caso y la gravedad de los hechos"[120].

[119] NOGUEIRA, H. (2005). Autodeterminación informativa y hábeas data en Chile e información comparativa. Anuario de derecho Constitucional latinoamericano, 2(11). p. 469.
[120] Artículo 23, inciso final de la Ley 19.628.

CAPÍTULO 5: Deficiencias en la Ley N°19.628

La Ley N°19.628, pese a regular la protección de los datos personales, no lo logra del todo, ya que dicha normativa contiene una serie de deficiencias, como, por ejemplo, la ley ante los avances tecnológicos se encuentra desactualizada, no se considera una autoridad de control independiente, el procedimiento de habeas data no es eficaz, falta de fiscalización y control, etc. Por tales razones, la Ley N°19.628 no logra cumplir su finalidad, la cual es proteger los datos personales de sus titulares.

Por otra parte, aunque se han realizado esfuerzos por parte del poder ejecutivo y legislativo para modificar la Ley N°19.628, las consultas públicas y los diálogos con expertos no han logrado resultados concretos.

Por lo tanto, se expone la necesidad de agilizar las modificaciones necesarias a la legislación de protección de datos que permita otorgar una mayor protección de los datos personales de sus titulares, tanto en su tratamiento, como en su utilización, etc., Lo anterior, con el objetivo de brindar mayor certeza jurídica con el fin de construir un marco jurídico más sólido. Por ende, las principales deficiencias que se deben considerar en la Ley N°19.628 son las siguientes.

5.1 Inexistencia de una autoridad independiente

En la Ley N°19.628:

> "Una de las graves deficiencias que adolece, desde su inicio, la regulación vigente sobre protección de datos personales fue la ausencia de una autoridad de control que tuviese competencias para que, en materia de tutela de datos personales, se capacite, recomiende, norme, fiscalice, resuelva casos y sancione los incumplimientos a la ley. Si bien nuestro país fue pionero en dictar una Ley de Protección de Datos Personales, en Latinoamérica, el resto de la región fue incorporando una autoridad de control ante la cual se pueda reclamar la protección de un derecho fundamental como es la autodeterminación informativa."[121]

En la actualidad, la falta de una autoridad competente encargada de fiscalizar y controlar el tratamiento de datos personales por parte de entidades privadas y organismos públicos es el principal obstáculo de nuestro marco regulatorio. Esto coloca a los titulares de datos en una posición

[121] CONSEJO PARA LA TRANSPARENCIA. (2017). Observaciones y propuestas del Consejo para la Transparencia. p.34. https://www.consejotransparencia.cl/wp-content/uploads/estudios/2019/01/Minuta-Observaciones-y-Sugerencias-Proyectos-de-Ley-de-Protecci%C3%B3n-de-Datos-.pdf

desfavorecida, ya que carecen de los recursos para abordar y resolver los conflictos relacionados con sus datos de manera efectiva.

En nuestro país, la posibilidad de establecer una autoridad independiente para la protección de datos ni siquiera fue discutida durante la tramitación de la Ley N°19.628. Solo se creó un registro de bancos de datos a cargo de organismos públicos, bajo la responsabilidad del Registro Civil, pero este no recibió facultades para requerir la inscripción de los organismos públicos, tampoco en caso de incumplimiento puede sancionarlos.

A diferencia de muchos países miembros de la Comunidad Europea, que deben cumplir con exigencias supranacionales, en Chile esta autoridad no existe. El Convenio 108 de Europa sobre protección de datos establece la obligación de crear una o más autoridades independientes para velar por el cumplimiento de los principios básicos de protección de datos y el flujo transfronterizo de los mismos.

La creación de estas autoridades de control se fundamenta en tres razones principales. En primer lugar, es necesario establecer mecanismos preventivos, ya que la vía judicial posterior a la violación de datos resulta insuficiente y poco adecuada en materia de protección de datos. En segundo lugar, se requiere una especialización técnica que estas entidades proporcionan. Por último, la independencia en el ejercicio de sus atribuciones y labores, exentas de influencias políticas o económicas.

5.1.2 Falta de fiscalización y control

La regulación chilena de datos personales carece de una entidad explícita para supervisar su cumplimiento. La ausencia de un organismo que controle y fiscalice la protección de datos es una deficiencia, llevando al Consejo para la Transparencia a asumir cierta supervisión en los organismos públicos, pero su alcance es limitado debido a la falta de autoridad fiscalizadora o sancionatoria. Además, el manejo de datos por parte de instituciones públicas y privadas carece de fiscalización, lo que genera desconfianza sobre su uso adecuado y puede tener implicaciones negativas en términos de crédito y empleo. La desconfianza se combina con el desconocimiento generalizado tanto de la normativa como de los derechos asociados, lo que también afecta a los tribunales de justicia. En resumen, se reconoce la necesidad de una entidad independiente de control en la legislación chilena de protección de datos, con un enfoque más expedito para los titulares y responsables de datos.

5.2 Falta de registros de bancos de datos privados

El artículo 22 de la ley establece que: "El Servicio de Registro Civil e Identificación llevará un registro de los bancos de datos personales a cargo de organismos públicos"[122]. Aunque se consideró la posibilidad de incluir los bancos de datos de particulares, esta idea fue descartada.

Por lo tanto,

> "no existe obligación por parte de los particulares de inscribir el banco de datos en algún registro que permita conocer con exactitud qué personas o instituciones están almacenando datos, toda vez que dicha obligación existe sólo para organismos públicos en los términos del Art. 22 de la Ley N°19.628 a manos del Servicio de Registro Civil, sin embargo, ante la omisión tampoco existe una sanción respectiva y el cumplimiento de la ley en este aspecto no ha sido homogéneo por parte de la administración, lo que representa un problema latente y preocupante debido a que es el Estado el principal tenedor de información personal por distintas razones (para efecto de planificación, gestión y orden público; para pronunciarse respecto de políticas públicas, etc.)."[123]

5.3 Críticas a la acción de habeas data

La acción contemplada en el artículo 16 de la Ley N°19.628, que busca proteger los datos personales, no logra la celeridad necesaria para enfrentar eficazmente a las vulneraciones de los titulares de los datos personales, ya que encontramos una serie de problemáticas que tiene la acción de habeas data, entre ellas:

> "las referidas a la determinación del tribunal competente; el desigual tratamiento procesal que tienen las partes en el proceso, lo que trae implícita la vulneración del debido proceso y la bilateralidad de la audiencia; y, finalmente, que no se establece un plazo de prescripción de la acción, con lo que se afecta también la seguridad jurídica."[124]

Esto ha llevado a que su uso no sea tan amplio como se esperaba inicialmente. Además, quienes se ven perjudicados por el mal uso de sus datos personales han preferido recurrir al recurso de protección

[122] Artículo 22, inciso primero de la Ley 19.628.
[123] KINDLEY, D. (2017). "El régimen de la Protección de Datos Personales en Chile: Análisis comparado, estándares internacionales y revisión crítica. El Derecho al Olvido y su tutela a través de la acción de Habeas Data". [Tesis de licenciatura, Universidad Austral de Chile], Repositorio institucional. p. 30. http://cybertesis.uach.cl/tesis/uach/2017/fjk.51r/doc/fjk.51r.pdf
[124] INSTITUTO CHILENO DE DERECHO Y TECNOLOGÍAS. (2017). De la no regulación de la protección de datos personales en Chile. Recuperado el 5 de julio de 2023 de https://www.icdt.cl/no-regulacion-de-datos-personales/

establecido en la Constitución para restaurar sus derechos y poner fin a acciones y omisiones injustas e ilegales, tanto por parte de entidades públicas como privadas.

El recurso de protección ofrece claras ventajas al abordar situaciones descritas en la Ley N°19.628. En primer lugar, es compatible con otras acciones, tanto administrativas como jurisdiccionales. Esto ha llevado a que la acción de habeas data se utilice de manera limitada. A diferencia de la acción especial de la ley, el recurso de protección no requiere representación legal y su procedimiento, aunque concentrado, es menos engorroso. Por un lado, a pesar de que la acción de habeas data permite solicitar indemnización por perjuicios, por otra parte, la celeridad y concentración del recurso de protección, lo convierten en la opción más adecuada en la actualidad.

El habeas data no ha tenido éxito en el país debido a su falta de capacidad para brindar respuestas rápidas en su procedimiento y mayor costo económico para sus titulares en comparación con el recurso de protección.

5.4 Exclusión de las personas jurídicas

La ley chilena excluye a las personas jurídicas como titulares de datos personales, ya que,

> "La aplicabilidad restringida de la ley a personas naturales encuentra fundamentos en ella misma, la propia letra ñ en su artículo segundo sostiene que para efectos de dicha ley es "titular de los datos, la persona natural a la que se refieren los datos de carácter personal". Corrobora lo anterior, lo dispuesto por la ley en comento en su Título V, acerca de las responsabilidad por infracciones, al señalar en su artículo 23: "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 (…)", nos parece que el artículo reafirma lo señalado por esta parte, toda vez que la jurisprudencia y doctrina se encuentran contestes respecto de que este tipo de daño es solo posible sufrir por personas naturales, más no por personas jurídicas."[125]

Sin embargo, una tendencia creciente en la doctrina y en numerosas leyes sobre la materia ha reconocido que las personas jurídicas pueden estar amparadas por estas leyes en cuanto a datos almacenados en bancos o registros. Es cierto que resulta difícil equiparar el derecho a la intimidad de las personas jurídicas con el de las personas físicas, ya que estas últimas sí tienen vida privada y honra, que tradicionalmente se ha considerado exclusiva de ellas. No obstante, las personas jurídicas, tanto civiles

[125] EL MERCURIO. (2 de enero de 2018). Datos personales y personas jurídicas: ¿Van de la mano?. Recuperado el 8 de julio de 2023, de https://www.elmercurio.com/legal/movil/detalle.aspx?Id=906232&Path=/0D/D3/

como comerciales, tienen datos e información que las identifican. Algunos de estos datos pueden ser considerados sensibles, además, muchas veces sus actividades gozan de notoriedad. Por tanto, no hay razones para excluir a las personas jurídicas de la regulación sobre datos personales.

5.5 Contradicción en el tratamiento de datos y el principio de finalidad

Existe una contradicción preocupante en la ley. Por un lado, el artículo 4 establece que las personas deben ser debidamente informadas sobre el propósito del almacenamiento y posible comunicación de sus datos personales. Sin embargo, el artículo 9 permite utilizar los datos para fines distintos a los que fueron recolectados si provienen de fuentes accesibles al público, sin necesidad de obtener consentimiento o informar al titular sobre esta nueva finalidad. Esto crea una situación peligrosa, ya que la definición amplia de fuentes accesibles al público hace que la obtención de datos de esta manera sea la norma. En estas circunstancias, los principios de consentimiento informado y tratamiento con fines específicos quedan sin aplicación.

5.6 Crítica a la definición de fuentes accesibles al público

En la actualidad, tratar datos personales por lo general requiere el permiso del titular, de acuerdo con el artículo 4. Sin embargo, se establece en el artículo 4, inciso quinto como excepción al consentimiento el tratamiento de datos personales que se recolecten o provengan de "fuentes accesibles al público", estos son:

> "registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes. Es decir, su consulta debe poder ser realizada por cualquier persona, como por ejemplo, los contenidos en diarios o en medios de comunicación social."[126]

Esto implica que cualquiera puede tratar información de estas fuentes. Hoy en día, cualquier información no confidencial se considera de acceso público. Internet, por ejemplo, es una fuente accesible al público, lo que podría permitir el tratamiento de datos personales sin consentimiento del titular, ni necesidad de una ley. Se critica este concepto de fuente accesible al público, ya que da al titular del registro o banco de datos la decisión de abrirlo al público, lo que puede llevar a posibles fraudes en el espíritu de la ley al permitir el tratamiento de datos sin autorización del titular.

[126] CONSEJO PARA LA TRANSPARENCIA. (s/f). Recomendaciones del Consejo para la Transparencia sobre protección de datos personales por parte de los órganos de la administración del Estado. p. 4. https://www.consejotransparencia.cl/wp-content/uploads/2020/01/RECOMENDACIONES-Para-organismos-del-Estado.pdf

5.7 Ineficacia de sanciones y multas

El artículo 16 establece sanciones que van de 1 a 50 unidades tributarias mensuales si se acepta una reclamación, dependiendo de la causal. Sin embargo, se ha criticado la falta de un régimen completo de infracciones y sanciones en la Ley, así como las "sanciones y multas de baja cuantía y hasta irrisorias"[127]. También, se cuestiona la falta de sanciones para entidades públicas o privadas que no informan a los afectados en caso de fuga de datos.

La ley no contempla sanciones penales contra quienes hagan un uso indebido o abusivo de datos personales en bancos o registros. Se ha señalado que limitar las sanciones solo al ámbito civil puede llevar a que el valor de las multas sea insignificante para grandes empresas que obtienen grandes ganancias de esta actividad. Sería conveniente aumentar las multas y, en caso necesario, considerar sanciones penales en relación con el tratamiento de datos personales en el Código Penal, junto con una normativa más completa sobre delitos informáticos.

Por último, La ley presenta deficiencias en cuanto a la responsabilidad, ya que las sanciones establecidas resultan ineficaces debido a que toda la carga probatoria recae en el titular de los datos. Esto significa que el titular, de manera enormemente onerosa, debe demostrar la culpa o negligencia del responsable de los datos. Esta situación dificulta y desfavorece la protección de los derechos de los titulares de datos frente a posibles infracciones.

La ausencia de una autoridad de control y la falta de un procedimiento de reclamación rápido contribuye a la impunidad de los infractores.

5.8 Falta de regulación al flujo internacional de datos

El legislador no reguló esta área, considerándola competencia de tratados internacionales. El artículo 5 permite que los responsables de bases de datos establezcan procedimientos automatizados de transmisión, sujetos a requisitos mínimos para proteger los derechos de los titulares y relacionarse con las tareas de los organismos, sin abordar la transmisión internacional de datos. Esta falta de regulación desvirtúa la Ley N°19.628 al permitir la transmisión sin regulación ni control adecuado de los datos.

Al no regularse, se permite la transmisión internacional siguiendo las disposiciones generales de la ley. Es discutible que el legislador haya omitido regular esto, dado que la realidad tecnológica muestra

[127] HERRERA, P. (2016). El derecho a la vida privada y las redes sociales en Chile. Revista chilena de derecho y tecnología, 5(1). p. 92.

que la fluidez internacional de datos crece diariamente, superando fronteras y generando conflictos sobre qué legislación aplicar.

Cabe señalar que, se lleva a cabo en la actualidad de "manera profusa este tipo de tratamiento de datos, que se sirve fundamentalmente de la Red Internet, tema que está absolutamente omitido en la Ley, haciéndose indispensable y urgente adaptarse a la normativa internacional que existe sobre la materia"[128].

5.9 Falta de protección de los datos sensibles

Es positivo que el concepto de dato sensible sea amplio, pero se critica la falta de ejemplos claros que establezcan cuándo un dato es sensible, la legislación actual no protege adecuadamente estos datos.

El artículo 10 establece que: "No pueden ser objeto de tratamiento los datos sensibles, salvo cuando la ley lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares"[129].

Entonces, se permite el tratamiento de datos sensibles sin consentimiento del titular si es necesario para beneficios de salud. Expertos critican esta excepción por abusos en la industria de la salud, utilizando esta norma más allá de su intención original.

5.9.1 Datos sensibles: Vacíos en pandemia

La crisis de COVID-19 ha revelado lagunas legales en el tratamiento de datos personales. La falta de reglas claras sobre seguridad y el tratamiento de datos sin consentimiento en emergencias resalta la vulnerabilidad en la protección de datos sensibles, como los datos de salud. La filtración de datos de COVID-19 muestra la fragilidad normativa. A pesar del derecho a la protección de datos establecido constitucionalmente en 2018, la ley está desactualizada. Las autoridades no han reconocido que los datos de contagios involucran información personal sensible protegida por la Constitución. Es esencial tratar estos datos bajo reglas estrictas para evitar su mal uso y daño a los afectados.

Cabe mencionar, que los datos de salud son datos sensibles, y que de acuerdo con la Ley N°19.628,

> "estos datos no pueden ser objeto de tratamiento, excepto si el titular consiente en ello, la ley lo autoriza o si es necesario para la determinación u otorgamiento de un beneficio de salud

[128] ROBERTS, R. (2018). Reporte: Consulta experta sobre la Ley de Protección de la vida Privada de las Personas. Biblioteca del Congreso Nacional de Chile. p. 9.
[129] Artículo 10 de la Ley 19.628

para su titular. En ningún momento esta ley señala razones de salubridad pública como causal para el tratamiento de datos sensibles."[130]

La Ley 20.584 establece que la información clínica solo puede ser accedida por personas involucradas en la atención médica. Además del titular, permite acceso a terceros autorizados notarialmente, fiscales, abogados con aprobación judicial. Por otra parte, los tribunales de justicia Ministerio y Servicios de Salud pueden acceder a dichos datos con fines estadísticos. La autorización basada en la protección de la salud solo aplica a organismos de salud, excluyendo a entidades estatales como policía o fuerzas armadas.

La Ley N°19.628 permite a los órganos estatales manejar datos personales en general, pero los datos sensibles, como fichas clínicas, tienen protección especial. La falta de autorización explícita para compartir estos datos con terceros, excepto según la Ley 20.584, impide a la policía, Fuerzas Armadas y municipios acceder a esta información. Esto es problemático en emergencias sanitarias, donde la comunicación de datos de salud entre entidades estatales es esencial.

5.10 Otras deficiencias en la Ley N°19.628

A) Falta de precisión en su ámbito de aplicación: Es relevante notar que la ley no excluye el tratamiento de datos personales domésticos ni el necesario para contratos laborales. Además, no aborda situaciones donde proveedores globales ofrecen servicios a personas en Chile desde fuera del país.

B) Falta de precisión del concepto de dato personal: La Ley define dato personal como cualquier información sobre personas naturales, identificadas o identificables. Sin embargo, ha recibido críticas por no ofrecer claridad para determinar si un dato es personal o estadístico (aquel que no puede ser vinculado a un titular identificado o identificable). Además, hay dificultad en definir el alcance de persona identificable.

C) Falta de ampliación del concepto de dato personal:

> "La aparición de nuevas tecnologías ha ampliado las formas de obtención de datos personales y de generación de información que permite identificar a una persona. Por ello una reforma a la ley debe contemplar un concepto amplio de dato personal que posibilite contener todos aquellos elementos identificables de un individuo."[131]

[130] CONTRERAS, P, y BORDACHAR, M. (25 de marzo de 2020). Pandemia y datos sensibles. CIPER Chile; Fundación CIPER. https://www.ciperchile.cl/2020/03/25/pandemia-y-datos-sensibles/

[131] FUNDACIÓN DATOS PROTEGIDOS. (s/f). Una propuesta a la ley de datos personales en Chile. p.19. https://datosprotegidos.org/wp-content/uploads/2017/11/InformeLeyDatos_FDP-3.pdf.

D) Falta de regulación del deber de información: Este problema es debido a la falta de control que tienen los titulares sobre sus datos debido a la abrumadora cantidad de información recopilada por diversas entidades. Esto lleva a que las personas desconozcan qué datos están siendo tratados, quiénes los administran y con qué propósito se recopilan, generando una situación de control deficiente para los titulares.

E) Falta de regulación del consentimiento: En la actualidad, la regulación del consentimiento abarca todos los tipos de datos por igual, lo cual ha sido cuestionado por expertos al no imponer requisitos más rigurosos para datos especialmente sensibles. Además, se genera incerteza jurídica al no aclarar cómo cumplir con la obligación de escriturar el consentimiento cuando se otorga en sistemas informáticos.

F) Falta de precisión del tratamiento de datos por personas jurídicas privadas: La excepción establecida en el inciso final del artículo 4 en el que no se requiere de autorización el tratamiento de datos personales que realicen las personas jurídicas privadas como se describe en dicho inciso, fue criticado debido a su redacción confusa y falta de contenido específico, lo que lleva a interpretaciones diversas y posibles abusos en su aplicación.

G) Falta de límites al tratamiento de datos por organismos públicos: La norma fue cuestionada por otorgar amplias facultades que constituyen una excepción al consentimiento, especialmente dada la importancia del Estado como recolector y procesador de datos personales.

CONCLUSIONES

La Ley N°19.628 que se inspiró en legislaciones europeas, ha sido un avance para proteger los datos personales de sus titulares, que a su vez protege este mismo derecho fundamental y la vida privada de las personas. El concepto de protección de datos personales engloba principios y normas sobre la recolección, almacenamiento, y tratamiento de datos de las personas. Este concepto ha evolucionado en sistemas jurídicos europeos para evitar la vulneración del derecho a la vida privada e intimidad de las personas mediante el mal uso de datos, por ello se originaron distintas legislaciones que protegen los datos personales. En 1999, Chile adoptó esta perspectiva a través de la Ley N°19.628. Sin embargo, esta ley necesita revisión debido al avance tecnológico y una serie de deficiencias que limitan la protección de los titulares y permiten la gestación de un tratamiento de datos sin supervisión ni control efectivo.

El desarrollo de la protección de datos personales se vuelve crucial debido a los avances tecnológicos, que exponen la privacidad de los usuarios a vulnerabilidades difíciles de percibir, ya que,

> "Los riesgos asociados al tratamiento de datos personales han aumentado por la emergencia de tecnologías de información tan complejas como el Big Data o la inteligencia artificial. Las tecnologías actuales permiten generar y procesar magnitudes increíbles de información personal y no solo circunscrita a datos recabados desde las plataformas digitales, sino que también desde nuestra propia biometría como las huellas dactilares o las huellas faciales. Por ello, la masificación de grandes volúmenes de información personal supone un gran reto para las legislaciones actuales, en cuanto a que estas tecnologías y sus algoritmos permiten la identificación de las personas, aun cuando esos datos son considerados anónimos o estadísticos."[132]

Por lo anterior, se requiere la creación de una normativa adecuada que se adapte al avance tecnológico y resguarde la protección de los datos de sus titulares en todas sus etapas.

Tanto Chile como el mundo han respondido a esta problemática mediante la creación de normativas para permitir a las personas controlar sus datos y evitar intromisiones de terceros, aunque en muchas ocasiones estas normativas son deficientes.

Cabe señalar que, las personas no suelen conocer sus derechos en relación con sus datos personales, y los encargados de manejar estos datos a menudo desconocen sus responsabilidades, esto se

[132] CONSEJO PARA LA TRANSPARENCIA. (s/f). La protección de datos personales en contextos de avanzado desarrollo tecnológico, con énfasis en videovigilancia y tecnología de reconocimiento facial empleada por el sector público. p. 6. https://www.consejotransparencia.cl/wp-content/uploads/2022/01/La-proteccio%CC%81n-de-datos-personales-en-contextos-de-avanzado-desarrollo-tecnolo%CC%81gico-con-e%CC%81nfasis-en-videovigilancia-y-tecnologi%CC%81a-de-reconocimiento-facial-empleada-por-el-sector-pu%CC%81blico-1.pdf

debe a la ausencia de campañas que promuevan la conciencia sobre la protección de los datos personales. La protección de datos personales en nuestro país sigue siendo un desafío no resuelto. Aunque se ha intentado discutir en el congreso, la falta de resultados efectivos se debe a la ausencia de un marco normativo sólido para garantizar una protección adecuada.

Carecemos de una legislación que cumpla con estándares internacionales para proteger los datos personales, la cual tiene innumerables falencias y se encuentra desactualizada. Los avances tecnológicos, especialmente internet, aumentan los riesgos al permitir la recolección y uso no autorizado de datos, incluso sin consentimiento del titular cuando los datos son de una fuente de libre acceso al público, lo que lleva a situaciones irregulares como la comercialización de datos.

En las áreas donde se estableció regulación, los titulares de datos quedaron en una posición vulnerable frente al Estado y las empresas que gestionan el tratamiento de datos. Las empresas (personas jurídicas privadas) tuvieron una influencia significativa en las etapas de discusión previas a la Ley N°19.628, incluso llegando a argumentar que los datos personales eran de su propiedad. Aunque esta idea fue eliminada, resalta la influencia de estas empresas durante el proceso. La amplitud de las situaciones exentas de requerir el consentimiento del titular para recolectar y tratar datos también ejemplifica cómo la falta de consentimiento se ha convertido en la norma, en lugar de la excepción.

La Ley N°19.628 ha colocado tanto al Estado como a las empresas en una posición favorable. Las empresas pueden tratar datos sin necesitar consentimiento si se ajustan a las normas que permiten su excepción, mientras que el Estado también puede hacerlo si se trata de asuntos de su competencia. Esto significa que la mayoría de nuestros datos pueden ser procesados sin nuestro conocimiento, con la excepción de los datos sensibles. Sin embargo, incluso aquí, existe una excepción, ya que se puede tratar estos datos sin consentimiento cuando se relacionen con el otorgamiento de beneficios de salud para sus titulares.

Los esfuerzos para mejorar la situación precaria de la legislación chilena han llevado a la presentación de varias iniciativas legislativas que proponen nuevos enfoques regulatorios. Sin embargo, ninguna de estas propuestas ha tenido éxito, ninguna de ellas incluye una autoridad de control independiente, única y especializada, con poderes como la supervisión y la imposición de sanciones. Además, ninguna de estas iniciativas ha abordado la cuestión desde una perspectiva que sea adecuada para la realidad chilena. En cambio, muchas de ellas son copias de sistemas europeos o simplemente reutilizan organismos con diversas funciones y competencias.

Es esencial destacar que la consagración constitucional del derecho a la protección de los datos personales carece de valor si la ley encargada de dar sustancia real a este derecho no cumple su función.

La actualidad nos muestra que una legislación mal concebida genera distorsiones y problemas significativos.

Por lo anterior, se proponen las siguientes modificaciones en la regulación establecida en la Ley N°19.628 en relación con la protección de los datos personales y también una serie de medidas a implementar con el objetivo de corregir estas deficiencias con el fin de resguardar efectivamente los datos personales de sus titulares:

La Ley N°19.628 establece principios clave sobre la protección de datos personales. Sin embargo, dada la rápida evolución de la sociedad, el comercio y la situación actual del país, esta legislación requiere una reforma profunda. Esto implica la creación de un organismo de control para garantizar la aplicación de principios fortalecidos, como el principio de finalidad de los datos, en línea con las directrices de la OCDE.

Se debe definir claramente el alcance de aplicación de las normas, excluyendo tratamientos de datos personales de carácter doméstico. También es necesario establecer en la Ley que esta será aplicable a servicios ofrecidos en Chile, incluso si el proveedor no está en el país.

Se debe mejorar las definiciones de dato personal y dato estadístico al agregar elementos que los diferencien claramente, y además aclarar la noción de persona identificable. Además, se debe ampliar el concepto de dato personal, incorporando elementos de los avances tecnológicos.

Se propone crear "un órgano con facultades y deberes de control, fiscalización, promoción e información de la protección de datos personales en Chile"[133], es decir, una entidad administrativa de control independiente con capacidad para imponer sanciones, autonomía y recursos propios. Además, se sugiere realizar fiscalizaciones periódicas y de oficio por parte de esta entidad, otorgarle la facultad de certificar códigos de autorregulación en diversas industrias, y desarrollar una política pública de difusión, capacitación y educación en protección de datos personales.

Se propone regular el deber de información, otorgándole control a los titulares sobre sus datos recopilado por diversas entidades. Los titulares deben tener conocimiento sobre los datos personales que están siendo tratados y qué entidad está realizando dicho tratamiento y con qué propósito.

[133] JIJENA, R., y CABALLERO, N. (8 de junio de 2021). Un órgano para la protección, el control, la fiscalización y la promoción del tratamiento de datos personales. Diario Constitucional. https://www.diarioconstitucional.cl/articulos/un-organo-para-la-proteccion-el-control-la-fiscalizacion-y-la-promocion-del-tratamiento-de-datos-personales/

Es necesario aclarar en la Ley N°19.628, en relación con el tratamiento de datos por organismos públicos, que la falta de autorización del titular para el tratamiento de datos está sujeta al principio de finalidad y se mantiene sujeto a las condiciones establecidas en el artículo 20.

Con respecto al habeas data se sugiere que los Juzgados de Policía Local podrían manejar casos relacionados con esta materia de manera más eficiente mediante un procedimiento abreviado y oral, aprovechando su experiencia en denuncias infraccionales y demandas sobre protección de derechos del consumidor. Se recomienda mantener como segunda instancia la Corte de Apelaciones.

Dadas las corrientes doctrinales, la inclusión de personas jurídicas como sujetos de protección de la protección de la Ley N°19.628 parece esencial. Aunque no poseen vida privada en el sentido constitucional, sí tienen una reputación que merece protección, similar a la otorgada a personas naturales. Además, dado que las bases de datos a menudo incluyen información sobre personas jurídicas, principalmente de naturaleza comercial, excluir su protección de la Ley N°19.628 resulta incoherente, ya que,

> ”consideramos que la confidencialidad y reserva de la información sobre las personas jurídicas es igualmente relevante como lo son de las personas naturales, al ser sujeto de derechos, y en su calidad de personas, merecen el resguardo y la protección de sus datos frente a posibles abusos de sus antecedentes propios o en el erróneo procesamiento de estos.”[134]

Es esencial establecer un registro de bases de datos gestionadas por particulares. Aunque no se busca supervisar todas las bases de datos privadas, se puede requerir el registro de aquellas a cargo de entidades financieras y comerciales debido a la vasta cantidad de información que tratan.

Se debe mejorar el registro de bases de datos gestionado por organismos públicos, tal como lo prescribe el artículo 22 de la ley. Esta disposición no otorga al Registro Civil las facultades necesarias para supervisar y sancionar la adecuada ejecución de su labor. Se requiere implementar capacidades de fiscalización para determinar si los organismos públicos han informado de manera correcta al Registro Civil sobre la creación de bases de datos, así como facultades sancionatorias en caso de incumplimiento de los términos definidos por el artículo 22.

Se debe establecer un sistema de sanciones proporcionales y coherentes con la conducta realizada y la multa correspondiente, por ello se propone la modificación del artículo 16, ajustando las

[134] GAJARDO, C., y MUNIZAGA, K. (2022). El Internet de las Cosas, ¿Una amenaza al Derecho a la Privacidad?. [Tesina, Universidad de Valparaíso]. p. 20-21. https://repositoriobibliotecas.uv.cl/bitstream/handle/uvscl/9367/TesinaGajardo%20y%20Munizaga.pdf?sequence=1&isAllowed=y

sanciones pecuniarias, reemplazando las sumas mínimas actuales por multas que ejerzan un efectivo incentivo al cumplimiento normativo. Se propone agregar un catálogo exhaustivo de infracciones con sanciones graduadas según su gravedad, junto con incentivos para informar a los titulares sobre posibles filtraciones de datos. Además, se sugiere establecer deberes y obligaciones distintos para quienes traten datos según su naturaleza.

Por otra parte, es necesario limitar las exenciones vinculadas a los datos obtenidos de fuentes públicas. Establecer una lista cerrada de fuentes consideradas públicas en la Ley para su uso en la normativa de protección de datos. Hay que aclarar que esta excepción aplica solo a ciertos tipos de datos y no como regla general. Además, es necesario modificar la definición genérica y ambigua de "fuentes accesibles al público" en el artículo 2, letra i). Sugerimos establecer una definición más precisa y enumerar taxativamente las excepciones para reducir su aplicación abusiva.

Reforzar el respeto al principio de finalidad en la normativa, incluyendo sanciones por su incumplimiento, por ello se propone que "el otorgamiento y obtención de datos sea utilizada en forma precisa para la finalidad para la cual fue entregada quedando impedido el responsable de datos darle cualquier otro uso sin contar con el consentimiento previo del afectado"[135].

Detallar con mayor precisión las situaciones en las cuales se puede aplicar la excepción al requerimiento de consentimiento en relación con el tratamiento de datos por las personas jurídicas privadas.

Revisar y mejorar la definición de datos sensibles considerando posibles discriminaciones futuras. Incluir datos de menores en esta categoría. Reforzar regulaciones sobre su tratamiento con consentimiento explícito, obligaciones detalladas y sanciones más fuertes. Aclarar el uso de la frase beneficios de salud en la ley. Regular reglas claras sobre seguridad y tratamiento de datos sensibles en emergencias sanitarias que puedan ocurrir, como lo fue la pandemia del COVID-19.

La actual ley no aborda la transferencia internacional de datos de manera específica, lo que implica que esta actividad se considera permitida siempre que se respeten las disposiciones generales de la ley. Sin embargo, sería beneficioso que la reforma incluyera regulaciones claras y precisas sobre este tema para facilitar el comercio internacional, por ello se propone su modificación, regulando detalladamente la transferencia internacional de datos.

[135] IBARRA, F. (s/f). Nociones fundamentales en protección de datos de carácter personal: teoría, práctica y actualidad. [Tesina, Universidad Alberto Hurtado]. p. 51. https://repositorio.uahurtado.cl/bitstream/handle/11242/7006/DERIbarra.pdf?sequence=1&isAllowed=y

Diferenciar el tipo de consentimiento en función del tipo de dato. Para datos sensibles, establecer un consentimiento expreso y previo, mientras que, para otros datos, considerar un consentimiento inequívoco. Imponer la obligación a quienes tratan datos de implementar mecanismos para un consentimiento claro e informado por parte de los titulares. Aclarar si el consentimiento otorgado mediante tecnologías informáticas cumple con el requisito de escritura.

Se sugiere agilizar la revisión de las modificaciones propuestas a la Ley N°19.628 para evaluar la necesidad de un cambio legislativo urgente. Esto busca adoptar un enfoque integral que protejan los principios de los datos personales, como la posible inclusión de una entidad de control independiente, en lugar de simplemente copiar modelos de otros países.

Se requiere de una política pública integral que respalde la implementación de la legislación adecuada, destine recursos suficientes para su ejecución y promueva campañas de concientización para informar a la población sobre sus derechos y los recursos disponibles para obtener apoyo.

Finalmente, la consolidación de un auténtico derecho a la protección de datos personales requiere una base teórica sólida y una legislación competente. Ambas deben estar desarrolladas adecuadamente para lograr los resultados deseados. Si ambas partes son deficientes, se generarán confusiones y se perjudicarán los derechos de las personas. La perspectiva de la presente memoria es centrada en la protección de los datos personales, ya que es primordial el resguardo de la vida privada de sus titulares. En esta línea, planteamos una visión a largo plazo que busca la implementación de una legislación integral. Por ello, se propone la modificación de la Ley N°19.628 y la implementación de una serie de medidas en donde efectivamente se incorporen los principios de protección de datos personales reconocidos por Chile.

Los desafíos que presenta la Ley N°19.628 no son insuperables. Por lo tanto, si hay una voluntad genuina de actualizar y mejorar la regulación actual sobre la protección de datos personales, tanto por los legisladores y los expertos, con el objetivo de modernizar la normativa y superar sus actuales deficiencias, no debería haber demora en presentar proyectos de reforma. Por lo mismo, el objetivo de esta memoria, tal como se ha descrito en los diversos capítulos de la presente memoria, es transmitir una noción global de la regulación establecida en la Ley N°19.628, sobre protección de los datos personales, permitiendo finalizar con la realización de una exposición y análisis de manera crítica de sus principales deficiencias, visibilizando la necesidad de modificar la Ley N°19.628 con el fin de mejorar la protección de datos personales. Sin embargo, es importante reconocer que mejorar la ley implica un equilibrio delicado entre fortalecer los derechos individuales de los titulares y considerar los intereses legítimos del Estado y las empresas dedicadas al tratamiento de datos personales.

BIBLIOGRAFÍA

Libros, Publicaciones y Tesis:

BARRIOS, V. (2018). Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de datos de Carácter personal y su Protocolo Adicional Relativo a las Autoridades de Control a los Flujos Transfronterizos de Datos. Biblioteca del Congreso Nacional de Chile.

BAZÁN, V. (2005). El hábeas data y el derecho de autodeterminación informativa en perspectiva de derecho comparado. Estudios Constitucionales. 3(2).

BERDUGO GÓMEZ DE LA TORRE, I. (1987). Honor y libertad de expresión. Madrid, Tecnos.

BUSTOS, J. (1992). Los límites de los derechos de libre expresión e información según la jurisprudencia, en García San Miguel, Luis: Estudios sobre derecho a la intimidad. Madrid, Tecnos.

CERDA, A. (2003). La autoridad de control en la legislación sobre protección frente al tratamiento de datos personales. [Tesis de Magíster, Universidad de Chile]. https://repositorio.uchile.cl/bitstream/handle/2250/106762/cerda_a.pdf?sequence=3&isAllowed=y

CERDA, A. (2012). Legislación sobre protección de las personas frente al tratamiento de datos personales. Santiago, Centro de Estudios en Derecho Informático, Universidad de Chile.

CONDE ORTIZ, C. (2005). La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad. Madrid, Dykinson.

CONTRERAS, P. (2020). El derecho a la protección de datos personales y el reconocimiento de la autodeterminación informativa en la Constitución chilena. Estudios constitucionales, vol 18(2).

DONOSO, L, y REUSSER, C. (2021). Protección de Datos Personales. Santiago. Ed, Academia judicial de Chile.

DRESNER, S. H. (1994). Panorama de la legislación europea sobre protección de datos personales. Informática y derecho: Revista iberoamericana de derecho informático, (6).

FAYOS GARDÓ, A., & CONDE COLMENERO, P. (2015). Los derechos a la intimidad y a la privacidad en el siglo XXI. Madrid, Dykinson.

GAJARDO, C., y MUNIZAGA, K. (2022). El Internet de las Cosas, ¿Una amenaza al Derecho a la Privacidad?. [Tesina, Universidad de Valparaíso].

https://repositoriobibliotecas.uv.cl/bitstream/handle/uvscl/9367/TesinaGajardo%20y%20Munizaga.pdf?sequence=1&isAllowed=y

GARRIDO, R. (2013). El Habeas data y la ley de protección de datos en Chile. Serie Bibliotecología y Gestión de Información, (83).

GARRIGA, A. (2016). Nuevos retos para la protección de datos personales: en la era del Big Data y de la computación ubicua. Nuevos retos para la protección de datos personales, Madrid, Dykinson.

HERRÁN, A. (2003). El derecho a la protección de datos personales en la sociedad de la información. España, Ed. Universidad de Deusto.

HERRERA, P. (2016). El derecho a la vida privada y las redes sociales en Chile. Revista chilena de derecho y tecnología, 5(1).

IBARRA, F. (s/f). Nociones fundamentales en protección de datos de carácter personal: teoría, práctica y actualidad. [Tesina, Universidad Alberto Hurtado]. https://repositorio.uahurtado.cl/bitstream/handle/11242/7006/DERIbarra.pdf?sequence=1&isAllowed=y

JARA, N. (2021). El derecho de propiedad sobre los datos. *Revista chilena de derecho privado*, (TEMATICO).

KINDLEY, D. (2017). "El régimen de la Protección de Datos Personales en Chile: Análisis comparado, estándares internacionales y revisión crítica. El Derecho al Olvido y su tutela a través de la acción de Habeas Data". [Tesis de licenciatura, Universidad Austral de Chile], Repositorio institucional. http://cybertesis.uach.cl/tesis/uach/2017/fjk.51r/doc/fjk.51r.pdf

LABBÉ, S. A., y LATRILLE, P. F. (2018). Protección de los datos personales en Chile, su tratamiento y comercialización. Análisis y críticas a la ley N° 19.628. [Tesis de licenciatura, Universidad Finis Terrae]. https://repositorio.uft.cl/xmlui/bitstream/handle/20.500.12254/1494/LABBE-LATRILLE%202018.pdf?sequence=1&isAllowed=y

LACRUZ, J. (1990). Elementos de derecho civil, I; Parte general del Derecho Civil, Volumen segundo, Personas, Barcelona, Ed. José María Bosch.

LEIVA, R. J. J. (1999). Dominios, marcas y comercio electrónico en internet: anexo: la nueva ley chilena sobre la no protección de datos personales, Nº 19628 del 28 de agosto de 1999. Informática y derecho: Revista iberoamericana de derecho informático, (30).

LOSANO, M. (1989). "Los orígenes de la Data Protection Act inglesa de 1984", en LOSANO, Mario, PÉREZ LUÑO, Antonio E., y GUERRERO MATEUS, Mª Fernanda.: Libertad informática y leyes de protección de datos personales, Madrid, Centro de Estudios Constitucionales.

LUCAS MURILLO DE LA CUEVA, P (1990). El derecho a la autodeterminación informativa. Madrid, Tecnos.

MARTÍNEZ DE PISÓN CAVERO, J. (1993). El derecho a la intimidad en la jurisprudencia constitucional. Madrid, Citas.

MEZA-LOPEHANDÍA, M. (2016). Libertad de expresión y protección de la intimidad: Chile, España y México. Santiago, Biblioteca del Congreso Nacional de Chile.

MUÑOZ, X.O.C. (1991). Libertad de expresión y sus límites: honor, intimidad e imagen. Madrid, Editoriales de Derecho Reunidas.

NAVARRETE, S. (2008). La protección de datos personales en Chile y la Ley N°19.628. [Tesis de licenciatura, Universidad Austral de Chile]. http://cybertesis.uach.cl/tesis/uach/2008/fjn321p/doc/fjn321p.pdf

NOGUEIRA, H. (2005). Autodeterminación informativa y hábeas data en Chile e información comparativa. Anuario de derecho Constitucional latinoamericano, 2(11).

NÚÑEZ, E. (2007). La importancia de la protección de datos de carácter personal en las relaciones comerciales. Aproximación al Derecho venezolano. Revista de derecho privado.

ORTIZ, P. J. (2003). Derechos del titular de datos y habeas data en la Ley N°19.628. Revista chilena de derecho informático, (2).

PASCUAL, P (2017). La génesis del derecho fundamental a la protección de datos personales. [Tesis Doctoral, Universidad Complutense de Madrid]. https://docta.ucm.es/rest/api/core/bitstreams/6ac257e3-656a-4aed-a4f2-c3b855c77cd7/content

PEÑA, S. A. (2019). Régimen de indemnización de perjuicios de la Ley N° 19.628 y la seguridad de datos personales. Análisis crítico del principio de seguridad de datos del artículo 11° de la Ley de protección a la vida privada y su aplicación práctica. [Tesis de licenciatura, Universidad de Chile]. https://repositorio.uchile.cl/bitstream/handle/2250/175622/Regimen-de-indemnizacion-de-perjuicios-de-Ley-no-19628-y-la-seguridad-de-datos-personales.pdf?sequence=1

REBOLLO, L. (2008). Vida privada y protección de datos en la Unión Europea. España, Dykinson.

ROBERTS, R. (2018). Reporte: Consulta experta sobre la Ley de Protección de la vida Privada de las Personas. Biblioteca del Congreso Nacional de Chile.

ROIG, A. (2009). E-privacidad y redes sociales. IDP: revista de Internet, derecho y política= revista d'Internet, dret i política, n°9. Barcelona, Universitat Oberta de Catalunya.

ROSENDE, H., RABAT, F., & WARNIER, M. (2013). Algunos alcances sobre la protección de los datos de carácter personal. Revista Actualidad Jurídica, Universidad del Desarrollo.

SILVA, A. C. (2003). Autodeterminación informativa y leyes sobre protección de datos. Revista Chilena de Derecho Informático, (3).

SILVA, J. W. (2001). Tratamiento de datos personales y protección de la vida privada. Universidad de los Andes.

TRAVIESO, J (2016). Protección de datos personales y tecnología. En busca del paraíso perdido. Revista tribuna internacional, vol 5, n°9.

VÁSQUEZ, E. E. (2004). El Hacking No Es (Ni Puede Ser) Delito. Revista Chilena de Derecho Informático, (4).

VIOLLIER, P. (2018). El Estado de la protección de datos personales en Chile. Derechos Digitales.

WILKINS, J (2014). Régimen legal nacional de protección de datos personales. Biblioteca del Congreso Nacional de Chile.

ZEGERS, I. (2021). La finalidad como estándar de protección de datos personales de carácter económico, financiero, bancario y comercial: un análisis desde la evolución normativa nacional y la regulación supranacional. [Tesis de licenciatura, Universidad de Chile]. https://repositorio.uchile.cl/bitstream/handle/2250/184367/La-finalidad-como-estandar-de-proteccion-de-datos-personales-de-caracter-economico.pdf?sequence=1&isAllowed=y

Páginas Web:

CONSEJO PARA LA TRANSPARENCIA. (2017). Observaciones y propuestas del Consejo para la Transparencia. https://www.consejotransparencia.cl/wp-content/uploads/estudios/2019/01/Minuta-Observaciones-y-Sugerencias-Proyectos-de-Ley-de-Protecci%C3%B3n-de-Datos-.pdf

CONSEJO PARA LA TRANSPARENCIA. (s/f). Formulario derecho ARCO. Recuperado el 17 de junio de 2023, de https://derechosarco.cplt.cl/Paginas/Inicio.aspx

CONSEJO PARA LA TRANSPARENCIA. (s/f). La protección de datos personales en contextos de avanzado desarrollo tecnológico, con énfasis en videovigilancia y tecnología de reconocimiento facial empleada por el sector público. https://www.consejotransparencia.cl/wp-content/uploads/2022/01/La-proteccio%CC%81n-de-datos-personales-en-contextos-de-avanzado-desarrollo-tecnolo%CC%81gico-con-e%CC%81nfasis-en-videovigilancia-y-tecnologi%CC%81a-de-reconocimiento-facial-empleada-por-el-sector-pu%CC%81blico-1.pdf

CONSEJO PARA LA TRANSPARENCIA. (s/f). Recomendaciones del Consejo para la Transparencia sobre protección de datos personales por parte de los órganos de la administración del Estado. https://www.consejotransparencia.cl/wp-content/uploads/2020/01/RECOMENDACIONES-Para-organismos-del-Estado.pdf

CONTRERAS, P, y BORDACHAR, M. (25 de marzo de 2020). Pandemia y datos sensibles. CIPER Chile; Fundación CIPER. https://www.ciperchile.cl/2020/03/25/pandemia-y-datos-sensibles/

ECIJA. (16 de noviembre de 2020). Tratamiento de datos personales por los organismos públicos en Chile. Recuperado el 20 de junio de 2023, de https://ecija.com/sala-de-prensa/tratamiento-de-datos-personales-por-los-organismos-publicos-en-chile/

EL MERCURIO. (2 de enero de 2018). Datos personales y personas jurídicas: ¿Van de la mano?. Recuperado el 8 de julio de 2023, de https://www.elmercurio.com/legal/movil/detalle.aspx?Id=906232&Path=/0D/D3/

FUNDACIÓN DATOS PROTEGIDOS. (s/f). Una propuesta a la ley de datos personales en Chile. p.19. https://datosprotegidos.org/wp-content/uploads/2017/11/InformeLeyDatos_FDP-3.pdf.

GDPR: LO QUE DEBES SABER SOBRE EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS. (s/f). Powerdata.Es. Recuperado el 27 de mayo de 2023, de https://www.powerdata.es/gdpr-proteccion-datos

INSTITUTO CHILENO DE DERECHO Y TECNOLOGÍAS. (2017). De la no regulación de la protección de datos personales en Chile. Recuperado el 5 de julio de 2023 de https://www.icdt.cl/no-regulacion-de-datos-personales/

JIJENA, R., y CABALLERO, N. (8 de junio de 2021). Un órgano para la protección, el control, la fiscalización y la promoción del tratamiento de datos personales. Diario Constitucional. https://www.diarioconstitucional.cl/articulos/un-organo-para-la-proteccion-el-control-la-fiscalizacion-y-la-promocion-del-tratamiento-de-datos-personales/

LA PROTECCIÓN DE LOS DATOS PERSONALES. (s/f). Europa.eu Recuperado el 15 de mayo de 2023, de https://www.europarl.europa.eu/factsheets/es/sheet/157/la-proteccion-de-los-datos-personales

MICROJURIS.COM CHILE. (18 de junio de 2018). Ley Nº 21.096 consagra constitucionalmente el Derecho a la Protección de datos personales. Noticias legales. Microjuris al Día Chile. Recuperado el día 5 de junio de 2023, de https://aldiachile.microjuris.com/2018/06/18/ley-no-21-096-consagra-el-derecho-a-la-proteccion-de-datos-personales/

NEHME, F. (s/f). Ejercicio de derechos ARCO y su tramitación. Recuperado el 15 de junio de 2023, de https://fn.cl/comunicaciones/ejercicio-de-derechos-arco-y-su-tramitacion

PODER JUDICIAL TV. (s/f). Reportaje Judicial: El recurso de habeas data y su aplicación en Chile. Recuperado el 23 de junio de 2023, de https://www.poderjudicialtv.cl/programas/reportaje/reportaje-judicial-el-recurso-de-habeas-data-y-su-aplicacion-en-chile/

PRIVACY ACT OF 1974. (16 de junio de 2014). Justice.gov. Recuperado el 13 de mayo de 2023, de https://www.justice.gov/opcl/privacy-act-1974.

REAL ACADEMIA ESPAÑOLA. Diccionario de la Lengua Española. Recuperado el 3 de mayo de 2023, de https://dpej.rae.es/lema/derecho-a-la-intimidad.

SEMPERE, J. (2012). XX Aniversario de la LORTAD: 20 años de Protección de Datos. Diario Jurídico Español, Madrid. Recuperado el 26 de mayo de 2023, de https://www.diariojuridico.com/xx-aniversario-de-la-lortad-20-anos-de-proteccion-de-datos/

SERNAC INVESTIGARÁ DENUNCIA CONTRA EQUIFAX POR INCUMPLIMIENTO DE LEY DICOM. (s/f). SERNAC: Noticias. Recuperado el 10 de junio de 2023, de https://www.sernac.cl/portal/604/w3-article-6696.html

SINOPSIS ARTÍCULO 18. Constitución Española. (s/f). Congreso.es. Recuperado el 30 de mayo de 2023, de https://app.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=18&tipo=2

TECNOWEB. (s/f). Ley de Datos Personales ARCO. Recuperado el 19 de junio de 2023, de https://www.tecnoweb.net/es-cl/ley-arco

Normativa Nacional:

CONSTITUCIÓN POLÍTICA DE LA REPÚBLICA DE CHILE. [C.P.], art. 20. 17 de septiembre de 2005 (Chile).

LEY N° 19.628, SOBRE PROTECCIÓN DE LA VIDA PRIVADA. (18 de agosto de 1999). Artículo 1, inciso primero. Diario Oficial de la República de Chile, Santiago.

LEY N° 19.812, MODIFICA LA LEY N°19.628, SOBRE PROTECCIÓN DE LA VIDA PRIVADA. (11 de junio de 2002). Artículo 1, numeral segundo. Diario Oficial de la República de Chile, Santiago.

Ley N° 20.285, Sobre acceso a la información pública. (11 de agosto de 2008). Artículo 33, letra m). Diario Oficial de la República de Chile, Santiago.

LEY N° 21.214, MODIFICA LA LEY N°19.628, SOBRE PROTECCIÓN DE LA VIDA PRIVADA, CON EL OBJETO DE PROHIBIR QUE SE INFORME SOBRE LAS DEUDAS CONTRAÍDAS PARA FINANCIAR LA EDUACIÓN EN CUALQUIERA DE SUS NIVELES. (24 de febrero de 2020). Artículo Único. Diario Oficial de la República de Chile, Santiago.

LEY N°21.504, ESTABLECE PROHIBICIÓN DE INFORMAR DEUDAS CONTRAÍDAS PARA FINANCIAR SERVICIOS Y ACCIONES DE LA SALUD EN LA LEY N°19.628. (4 de noviembre de 2022). Artículo Único. Diario Oficial de la República de Chile, Santiago.

Normativa Internacional:

ONU: ASAMBLEA GENERAL. (1948). Declaración Universal de los Derechos Humanos. (217 [III] A). Paris. Recuperado el 15 de abril de 2023, de http://www.un.org/en/universal-declaration-human-rights/

PRINCIPIOS RECTORES PARA LA REGLAMENTACIÓN DE LOS FICHEROS COMPUTADORIZADOS DE DATOS PERSONALES Adopción: Asamblea General de la ONU Resolución 45/95, 14 de diciembre de 1990 Las modalidades de aplicación de los reglamentos relativos a los ficheros computadorizados de datos personales se dejan a la libre iniciativa de cada Estado con sujeción a las siguientes orientaciones: A. PRINCIPIOS RELATIVOS A LAS GARANTÍAS MÍNIMAS QUE DEBERÍAN PREVERSE EN LA LEGISLACIÓN NACIONAL. (s/f). Gob.mx. Recuperado el 20 de mayo de 2023, de http://www.ordenjuridico.gob.mx/TratInt/Derechos%20Humanos/OTROS%2015.pdf