EVALUACIÓN DE LA LEY
CÁMARA DE DIPUTADOS CHILE

EVALUACIÓN DE LA LEY N°19.628

Protección de la Vida Privada.

COMITÉ EVALUACIÓN DE LA LEY/OCDE

CÁMARA DE DIPUTADOS DE CHILE

Lorenzini Basso, Pablo (Presidente)

Ceroni Fuentes, Guillermo

Gutiérrez Gálvez, Hugo

Gutiérrez Pino, Romilio

Kort Garriga, Issa

Monsalve Benavides, Manuel

Pérez Lahsen, Leopoldo

Robles Pantoja, Alberto

Sepúlveda Orbenes, Alejandra

Agosto de 2016

Departamento de Evaluación de la Ley
Camila Fauré Sánchez
Maryan Henríquez Ayala
Paulina Maturana Arancibia
Mauricio Pérez (Colaborador)

René Arrayet Pinto

PRESENTACIÓN PRESIDENTE DE LA CÁMARA DE DIPUTADOS DE CHILE

Nuestro país cuenta con un marco normativo de protección de datos personales que data de 1999, momento en que las tecnologías de la información y las relaciones económicas y sociales corrían con una velocidad y dinamismo diferente al que vivimos en la actualidad. Este escenario, ha introducido nuevas exigencias para la protección de derechos, entre ellos los referidos a la información personal e intimidad.

Buena parte de las acciones que realizamos a diario están sujetas a la constante entrega de datos personales, sin embargo, no es posible determinar con certeza si la información aportada está siendo utilizada para los fines consentidos, quiénes son los responsables del tratamiento de los datos y si la información sensible está lo suficientemente protegida ante posibles fugas o fallos informáticos.

Chile fue pionero en Latinoamérica en la generación de un marco regulatorio en datos personales, no obstante, esta legislación debe adaptarse a los estándares internacionales y proporcionar una cobertura suficiente que contemple una institucionalidad activa y un marco sancionatorio que de garantías de su correcta aplicación.

Por tanto, se hace necesario y urgente robustecer una norma tan trascendental para los tiempos que corren como es la Ley N°19.628. Así lo ha entendido la Cámara de Diputados, que a través del Departamento de Evaluación de la Ley pone a disposición de la ciudadanía y los legisladores material que permite dar cuenta del desconocimiento transversal que tanto instituciones públicas, privadas y usuarios tienen sobre la materia, además de los nudos críticos que impiden efectuar una correcta fiscalización y control sobre la aplicación e implementación de la norma.

Para avanzar hacia una norma más sólida en materia de protección de datos personales, se requiere de un compromiso de los distintos actores involucrados que permita generar un marco institucional y normativo que dé garantía de un tratamiento adecuado de la información personal.

PRESENTACIÓN PRESIDENTE COMITÉ DE EVALUACIÓN DE LA LEY /OCDE

Chile se encuentra al debe en materia de protección de datos personales. Esto es un hecho. Existe consenso en que transcurridos 17 años desde la publicación de la Ley N°19.628 las normas internacionales y los mercados exigen garantías en el tratamiento de datos personales, cuya falta que puede llegar a establecer barreras para el crecimiento del país, situación a la que nuestro país se ve enfrentado actualmente.

El Comité de Evaluación de la Ley/OCDE que presido y que se encuentra conformado por nueve Diputados de distintas bancadas, ha querido retomar el debate legislativo sobre la protección de datos personales, a través de esta herramienta de fiscalización que es la Evaluación de la Ley, de manera de conocer las debilidades de la norma vigente y los caminos para su modificación.

Desde el año 2009, se viene realizando desde el ejecutivo una serie de iniciativas, encuentros, consultas públicas, con diversos actores involucrados para generar acuerdos sobre la materia, sin embargo, éstos no se han concretado en un proyecto de ley que entregue mayores garantías tanto para los dueños de los datos como para quienes los tratan.

La Organización para la Cooperación y el Desarrollo Económico (OCDE) ha reiterado la necesidad de que nuestro país cuente con un marco normativo más sólido, por lo que en un acto inédito y a la luz de este estudio realizado por la Cámara de Diputados, desarrollamos instancias de diálogo con el Poder Ejecutivo, concretamente con el Ministerio de Hacienda y Economía, para dar respuesta a esta exigencia.

El informe que presentamos a continuación, reúne años de experiencia internacional, analiza el marco normativo y recoge el testimonio de profesionales de organismos públicos, especialistas, organizaciones sociales, gremiales y de consumidores, con el fin de aportar a la discusión legislativa datos relevantes para encontrar un camino que, en definitiva, otorgue el marco legal que nuestro país necesita para la protección de datos personales.

H.D. PABLO LORENZINI B.
Presidente
Comité de Evaluación de la Ley

TABLA DE CONTENIDOS

INTRODUCCIÓN

Los datos personales en la era de la información juegan un papel central para la industria del desarrollo tecnológico. Iniciativas como el Big Data o tratamiento masivo y automatizado de bases de datos (Velasco y Viollier, 2016), Cloud Computing o información guardada en la nube, la presencia de objetos como relojes inteligentes o internet de las cosas, junto a la telefonía móvil y las redes sociales, forman un escenario que se nutre de bases de datos cuyo tratamiento y protección han sido objeto de un cuestionamiento transversal de los actores involucrados en la materia.

Sin embargo, la industria tecnológica es solo una parte del sistema que utiliza datos personales para su funcionamiento. En el día a día cientos de instituciones públicas y privadas están requiriendo de información de esta índole para entregar servicios tan básicos como una compra en el supermercado o farmacia, la venta de un bono para una consulta médica, adquisición de seguros, hasta la elaboración de políticas públicas por parte del Estado.

¿Está nuestro país preparado para entregar garantías de un tratamiento de datos personales al nivel que lo exigen las normas internacionales y el desarrollo tecnológico? ¿Cuenta Chile con una institucionalidad capacitada para velar, fiscalizar y resolver cuando se genera un mal uso de la información proporcionada por los titulares de los datos? Finalmente, ¿Son suficientes y expeditas las herramientas que establece la norma vigente en protección de datos para que un ciudadano pueda ejercer su derecho a reclamación si así lo desea? Estas son algunas de las preguntas que orientaron la investigación que a continuación se pone a disposición de los legisladores y la ciudadanía.

La Evaluación de la Ley N°19.628 sobre protección de la vida privada recoge parte del debate público en torno al tratamiento de datos personales, desarrollado en nuestro país con fuerza en los últimos diez años. Varios han sido los intentos por mejorar la regulación nacional en esta materia, los que han posibilitado, inclusive, grandes consensos entre representantes de instituciones públicas, académicos expertos y gremios. No obstante, estos no se han concretado en cambios legislativos ni institucionales.

El presente informe considera la normativa internacional de protección de datos personales, la legislación extranjera, el marco normativo de la Ley N°19.628 y el control y fiscalización de la norma, con el fin de proporcionar -a partir del análisis jurídico y de los testimonios de los actores involucrados- conclusiones y recomendaciones que permitan complementar el debate legislativo una vez ingresado el proyecto de ley por parte del Poder Ejecutivo.

CAPÍTULO I. ANTECEDENTES DE LA EVALUACIÓN DE LA LEY N°19.628

La Ley N°19.628 tuvo su origen en una Moción del Senador Eugenio Cantuarias en enero de 1993. Luego de 6 años de tramitación, fue publicada el 28 de agosto de 1999. Posteriormente, fue modificada por las Leyes N° 19.812, 20.463, 20.521 y 20.575, esta última en el año 2012.

Su principal propósito fue llenar el vacío manifiesto que existía en nuestro ordenamiento jurídico, de modo de otorgar protección al derecho a la privacidad de las personas, en el ámbito del Derecho Civil, ante eventuales intromisiones ilegítimas.

Los principales parámetros orientadores del proyecto fueron:

- La Declaración Universal de Derecho Humanos de 1948
- La Declaración Americana de los Derechos y Deberes del Hombre de 1949
- El Pacto Internacional de Derecho Civiles y Políticos de 1966
- La Convención Americana sobre Derechos Humanos de 1969
- El mandato constitucional de los artículos 5° y 19° números 4 y 5 de nuestra Carta Fundamental.

Dentro de los objetivos del Proyecto, cabe destacar:

- Abordar las propuestas legislativas de protección civil que resulten necesarias para dar debida satisfacción al mandato constitucional.

- Diseñar mecanismos de protección frente a las intromisiones ilegítimas de que puede ser objeto la vida privada y los instrumentos de compensación ante los eventuales daños morales y materiales que se produzcan con ocasión de estas.

1. POBLACIÓN OBJETIVO O DESTINATARIA

La Ley N°19.628 busca otorgar el marco jurídico aplicable al tratamiento de los datos personales en registros o bancos de datos, tanto por organismos públicos como particulares. En este sentido, el público destinatario de la norma es toda persona que efectúe tratamiento de datos personales y los titulares de estos datos.

2. HERRAMIENTAS DE LA LEY N°19.628

- Regulación de la utilización de datos personales, disponiendo expresamente los supuestos en los cuales esto es posible.
- Establecimiento de un catálogo de derechos para los titulares de los datos, dentro del cual se incluye el derecho a exigir a quien sea responsable de un banco información sobre el propósito del almacenamiento y a quién se transmite dicha información; a solicitar su eliminación, bloqueo o modificación, en los casos que corresponda.
- Consagración de un procedimiento de amparo a los derechos señalados precedentemente ante el juez civil.
- Regulación de la utilización de datos relativos a obligaciones de carácter económico, financiero, bancario o comercial, a través de la mención expresa de los casos en que puede comunicarse dicha información.
- Establecimiento de la responsabilidad de ciertas infracciones y sus sanciones, tanto para personas naturales o jurídicas privadas, como para organismos públicos.
- Incorporación de una norma en el Código Sanitario que consagra la reserva de las recetas médicas y análisis o exámenes de laboratorios clínicos y servicios relacionados con la salud.

3. REGLAMENTO DE LA LEY N°19.628

De conformidad a lo señalado en el artículo 22° de la Ley, el Servicio de Registro Civil e Identificación debe llevar un registro de los bancos de datos personales a cargo de organismos públicos. Cumpliendo con el mandato legal, el Decreto N°779 publicado el 11 de noviembre del año 2000, aprueba el Reglamento de bancos de datos personales a cargo de organismos públicos.

4. SOLICITUD DE EVALUACIÓN DE LA NORMA

El Comité de Evaluación de la Ley/OCDE, en sesión N°9 celebrada el día miércoles 13 de enero de 2016, solicitó al Departamento la Evaluación de la Ley N°19.628 sobre protección de la vida privada, atendiendo a la especial recomendación que la OCDE realizara a nuestro país al momento de ingresar a dicho organismo internacional, de adecuar la normativa vigente a los estándares internacionales de protección de la vida privada y flujo transfronterizo de datos.

De esta manera, el Comité estableció como primera necesidad estudiar la normativa con el fin de aportar a su discusión legislativa con antecedentes concretos sobre su implementación, en vías de modificar la norma a partir del proyecto de ley que desde el Poder Ejecutivo se envíe al Congreso.

5. OBJETIVO DEL ESTUDIO

La investigación tuvo como eje central evaluar el marco jurídico y la implementación de la normativa vigente, con especial énfasis en temas que han sido de alto interés en el debate público y legislativo. Para lo anterior, el estudio se focalizó en las siguientes líneas investigativas:

- Adecuación de Ley a la normativa internacional vigente
- Institucionalidad para la adecuada protección de los datos personales
- Eficacia del procedimiento de reclamación o amparo

6. DESCRIPCIÓN METODOLÓGICA

La evaluación de la Ley N°19.628 fue realizada en base a la metodología diseñada por el Departamento y respaldada por la OCDE, que plantea el proceso de investigación a partir de tres fases: Estudio Técnico de la Ley, Percepción Ciudadana y Elaboración del Informe.

El estudio técnico consideró el análisis jurídico de la Ley y la normativa asociada, los instrumentos elegidos por el legislador para alcanzar los objetivos y la institucionalidad vigente. Del mismo modo, analizó la regulación internacional sobre el flujo y tratamiento de datos personales, debido a la relevancia que cobran las declaraciones y pactos de organismos internacionales, así como la legislación comparada.

Otra de las materias que se aborda en esta primera fase, guarda relación con la identificación de las instituciones involucradas en la implementación de la norma, el rol que estas desempeñan, los principales beneficiarios y/o afectados por la Ley y los posibles efectos no previstos por el legislador. En base a lo anterior, se determina el objetivo del estudio.

Es importante señalar que la metodología debe adaptarse a los requerimientos y especificaciones de cada norma a evaluar, que en el caso particular de la Ley de Protección de la Vida Privada, debió considerar el nivel técnico que contiene la misma.

Por lo anterior, la primera fase de estudio se llevó a cabo a través de entrevistas semi-estructuradas aplicadas a expertos en el tratamiento de datos personales y representantes de instituciones públicas asociadas a la temática. Cabe destacar que la percepción ciudadana, que habitualmente se trata como una fase independiente y que se recoge a través de la participación de organizaciones sociales especializadas en la materia a evaluar, tuvo un rol fundamental en esta primera fase por considerarlos como actores relevantes en el debate público y por el nivel de especialización y conocimiento que estas poseen sobre la materia en comento.

ENTREVISTADOS PARA LA EVALUACIÓN

Se realizaron un total de diez entrevistas, en el que participaron las siguientes instituciones y especialistas:

Consejo para la Transparencia

- Andrea Ruiz R. - Directora Jurídica
- Pablo Contreras V. - Jefe Unidad Normativa y Regulación
- Leslie Montoya R. - Abogada Unidad de Normativa y Regulación
- J. Eduardo Baeza P. - Abogado Unidad de Normativa y Regulación

Servicio Nacional del Consumidor (SERNAC)

- Andrés Herrera - Subdirector Jurídico y de Consumo Financiero

Centro de Estudios en Derecho Informático (CEDI)

- Alex Pessó S. - Coordinador Académico
- Rodrigo Moya G. - Académico e Investigador

Instituto Chileno de Derecho y Tecnología

- Lorena Donoso A. - Presidenta

Fundación Datos Protegidos

- Romina Garrido I. - Presidenta
- Jessica Matus A. - Directora

Organización Derechos Digitales

- Juan Carlos Lara - Director de investigación y políticas públicas
- Pablo Viollier - Analista de Políticas Públicas

Especialistas en Protección de Datos Personales

- Carlos Reusser - Académico y especialista en Derecho Informático
- Raúl Arrieta - Ex asesor del Ministerio de Economía
- Nicolas Yurazeck - Abogado estudio Garcia Magliona & Cia.
- Flavio Quezada - Académico Constitucionalista

En una segunda fase de la investigación, se invitó a participar a organizaciones de consumidores para que expresaran su opinión sobre la Ley y propusieran medidas para mejorar el conocimiento de la ciudadanía tanto de la norma como de las herramientas contempladas para denunciar el mal uso de sus datos personales. En dicha oportunidad, se realizó una reunión conjunta en la que participó el Presidente de la Organización de Consumidores y Usuarios de Chile (ODECU), Stefan Larenas y el Vicepresidente de la Corporación Nacional de Consumidores y Usuarios de Chile (CONADECUS), Sergio Donoso.

Adicionalmente, se realizaron dos focus group integrados por representantes de organizaciones gremiales de diversos sectores productivos y de servicios, con el objetivo de conocer su percepción sobre la norma y su implementación, además de escuchar sus propuestas para potenciar la regulación vigente.

NOMBRE GREMIO	REPRESENTANTE
Asociación de Bancos e Instituciones Financieras (ABIF)	Luis Cordero, Abogado
Asociación de Aseguradores de Chile A.G. (AACH)	Cristián Millán, Gerente de Operaciones Francisco Serqueira, Abogado
Asociación Gremial de AFP (AAFP)	Fernando Larraín, Gerente General
Cámara de Comercio de Santiago (CCS)	Cristián García-Huidobro, Secretario General Alejandra Velasco, Abogada
Comité Retail Financiero	Claudio Ortiz, Vicepresidente Ejecutivo Eduardo Escalona, Asesor
Federación Chilena de Asociación de Innovación y Tecnologías (FEDIT)	Rodrigo Bustamante, Abogado Directorio
Asociación de Empresas de Digitalización y Gestión Documental (DIGITAL AG)	Francisco Rivas, Presidente Microsystem
Asociación de Mutuales A.G.	Ernesto Evans, Consultor y Presidente
Cámara Chilena Norteamericana de Comercio (AMCHAM)	Tatiana Molina, Gerente de Contenidos Paulina Silva, Abogado Elias Mohor, Abogado
Asociación de ISAPRES	Gina Peri, Abogada
Asociación Investigadores de Mercado (AIM Chile)	Elvira Chadwick, Miembro Directorio
Asociación de Marketing Directo y Digital de Chile (AMDD)	Rodrigo Edwards, Presidente del Comité de Regulación
Asociación Chilena de Agencias de Publicidad (ACHAP)	Jorge Jarpa, Gerente General
Cámara Nacional de Comercio, Servicios y Turismo de Chile (CNC)	Nicole Kuppenheim, Ejecutiva Gremial Sebastián Hurtado, Abogado Nicolás Yuraszeck, Abogado

Finalmente, el proceso de Evaluación de la Ley culmina con la publicación de un informe que recoge el análisis efectuado en las fases anteriores, además de incorporar conclusiones y recomendaciones tendientes a proponer nuevos antecedentes que aporten a la discusión legislativa sobre la materia evaluada. El informe es publicado íntegramente en el sitio web del Departamento de Evaluación de la Ley, www.evaluaciondelaley.cl, quedando a disposición del público interesado.

7. DOCUMENTOS APORTADOS POR ENTIDADES EXTERNAS A LA EVALUACIÓN DE LA LEY

Para la evaluación de la Ley N°19.628 instituciones externas aportaron con análisis y estudios sobre la norma, elaborados especialmente para esta investigación.

El Servicio de Registro Civil e Identificación participó mediante oficio, a solicitud de este Departamento, con información relevante sobre la aplicación del artículo 22° de la Ley N°19.628 que encomienda al Servicio llevar el registro de banco de datos personales a cargo de organismos públicos.

El documento da cuenta del procedimiento de inscripción en el registro e incorpora una nómina que desglosa por año las instituciones informantes y el total de bancos de datos asociados a la institución. Así mismo, describe la experiencia obtenida durante los años a cargo del mismo.

El Consejo Para la Transparencia, entregó dos documentos en que analiza la norma y propone medidas correctivas para mejorar su marco legal e implementación. El primero lleva por nombre *Principales falencias en la normativa contenida en la Ley N°19.628 sobre protección de la vida privada* y detalla antecedentes, en el que se realiza un análisis de las principales dificultades o brechas contenidas en la norma, además de presentar conclusiones.

En el segundo documento titulado *Propuesta General de Perfeccionamientos normativos en materia de protección de datos personales*, el Consejo detalla diez propuestas tales como consagrar la autodeterminación informativa como derecho fundamental y objeto de protección de la Ley N°19.628, incorporar principios rectores, reforzar la regulación del consentimiento expreso e informado, regular el flujo transfronterizo de datos, el tratamiento de datos por organismos públicos, entre otros. Además, integra un análisis y propuesta para el establecimiento del Consejo Para la Transparencia y protección de datos, en el que se establece un objeto, estructura, régimen de designación y remoción, régimen de inhabilidades, incompatibilidades y tratamiento de intereses, régimen de funcionamiento y las funciones y atribuciones que asumiría el nuevo órgano.

La Cámara de Comercio de Santiago en el documento *Evaluación de la Ley N°19.628 sobre Protección de Datos Personales y propuestas de perfeccionamiento* señala su experiencia con la norma como administrador del Boletín de Informaciones Comerciales y expone una serie de falencias y propuestas para modificarla.

La Cámara Chilena Norteamericana de Comercio (AMCHAM CHILE) aportó con una *Minuta de Presentación* en la que entrega su opinión sobre la norma, con especial énfasis en lo referido al régimen de excepciones, los requisitos para el consentimiento, extensión de las excepciones y propuestas de modificación para los mismos.

El Comité de Retail Financiero resumió su opinión sobre la norma a través de un escrito en el que se refiere a la gestión de datos que las empresas que integran el comité efectúan, además de exponer los principales problemas de la Ley y entregar propuestas para realizar mejoras que consideraron como urgentes, vinculadas al ámbito de aplicación de la norma, al principio de finalidad, la implementación de una institucionalidad y la necesidad de implementar gradualmente la reforma.

El académico y abogado especialista en derecho Informático, Alberto Cerda Silva, elaboró el documento titulado *Legislación sobre protección de las personas frente al tratamiento de datos personales*, en abril de 2012, trabajo que fue aportado a esta investigación por el Centro de Estudios en Derecho Informático. La publicación, contiene un análisis crítico sobre protección de datos personales, en el que incorpora temas como la autodeterminación informativa y legislación y una revisión exhaustiva de la Ley N°19.628.

CAPÍTULO II. CONTEXTO INTERNACIONAL

Existe una serie de convenios y directrices emanados por organismos internacionales que han trazado, desde la década de los ochenta, diversos lineamientos para establecer un adecuado tratamiento de datos personales.

En este capítulo se realiza una revisión en tres fases sobre las tendencias existentes en la normativa internacional, destacando el tránsito desde los enfoques centrados en el derecho a la vida privada, pasando hacia una norma que releva la importancia de los datos personales, hasta llegar a las directrices y estándares que avanzan hacia la concepción de la protección de datos personales como un derecho en sí mismo.

Por otra parte, se revisa la legislación extranjera vigente, adentrándonos en la experiencia y enfoques que algunas naciones han efectuado y que le ha permitido posicionarse como modelo de buenas prácticas. Se destacan, por tanto, la experiencia de legislaciones como la de la Unión Europea, España y Uruguay.

1. NORMATIVA INTERNACIONAL

La comunidad internacional, con el transcurso de los años, ha generado distintas iniciativas para regular el flujo de datos personales o, al menos, establecer ciertos estándares mínimos. Así, se consideran las políticas, declaraciones, directrices y resoluciones de distintos organismos internacionales que se refieren al tratamiento de datos personales, los que fueron clasificados en tres etapas atendiendo la concepción del derecho a la protección de datos que refleja el documento.

a. Primera Etapa

Se caracteriza por referirse únicamente al derecho a la vida privada, sin considerar la protección de los datos personales como un derecho autónomo. Se trata de los primeros reconocimientos internacionales a la vida privada como tal, donde destacan:

- La Declaración Universal de los Derechos Humanos adoptada y proclamada por la Asamblea General de la Organización de las Naciones Unidas en el año 1948, reconoce un catálogo de derechos inherentes a la persona humana dentro de los que se incluye el derecho a la vida privada y a la honra.
- La Declaración Americana de Derechos y Deberes del Hombre, aprobada por la IX Conferencia Internacional Americana en el año 1948 (Organización de los Estados Americanos), reconoce el derecho a la vida privada y la honra de todos los individuos.
- El Pacto Internacional de Derechos Civiles y Políticos, aprobado por la Asamblea General de la Organización de las Naciones Unidas en el año 1966, reitera el deber de protección de los estados a la vida privada de los individuos.
- La Convención Americana sobre Derechos Humanos, suscrita en la Conferencia Especializada Interamericana sobre Derechos Humanos (Organización de los Estados Americanos) en el año 1969, reafirma la protección a la vida privada y la protección que debe otorgar la ley para evitar injerencias en la esfera de intimidad de las personas.

b. Segunda Etapa

Se observa un nuevo derecho que se desprende de la vida privada, formándose el derecho a la protección de datos personales. Se lo reconoce más bien desde un criterio económico, centrado principalmente en la transacción internacional de datos (datos transfronterizos), lo que dice estrecha relación con el carácter económico de los organismos internacionales que se pronuncian al respecto.

- Las Directrices sobre Protección de la Privacidad y Flujos Transfronterizos de Datos Personales de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) del año 1980.

La OCDE fue el primer organismo internacional en tratar el tema de la protección de datos personales, siendo una innovación al observar el tratamiento de datos más allá de la mera privacidad. Se enfocó en generar estas directrices en base a los tres principios que agrupan a los estados que conforman esta institución: la democracia pluralista, el respeto de los derechos humanos y las economías de mercado abiertas.

Estas directrices se caracterizan por tener un alto grado de flexibilidad y claridad, con el objetivo de facilitar su adaptación ante el avance tecnológico.

En su prólogo, evidencia su visión económica, pues hace referencia a que estas directrices buscan solucionar disparidades en las legislaciones nacionales y que suponen un obstáculo a la libre circulación de datos transfronterizos. Obstáculo que afectaría a la industria de la banca y los seguros.

Este documento define lo que se entenderá por datos personales y por circulación transfronteriza de datos personales. Señalando que su ámbito de aplicación es el sector público y privado.

También genera un catálogo de principios de aplicación nacional, donde destacan el principio de consentimiento, de calidad, finalidad, seguridad y responsabilidad. Estos conforman el elemento central en la protección de datos personales. Igualmente genera principios para el flujo transfronterizo de datos, donde destaca la libre circulación de estos.

Impone a los estados miembros la necesidad de adoptar procedimientos o instituciones jurídicas, administrativas u otras para la protección de la intimidad y de las libertades individuales respecto a los datos personales.

En esta fase también se encuentran los siguientes instrumentos:

- La Declaración sobre Flujos de Datos Transfronterizos fue pronunciada por la Organización para la Cooperación y el Desarrollo Económicos en el año 1985, y abordaba las cuestiones políticas que surgían del flujo de datos personales más allá de las fronteras nacionales como flujos de datos e información sobre actividades comerciales, flujos intraempresariales, servicios de información informatizada, e intercambios científicos y tecnológicos.
- La Declaración Ministerial sobre la Protección de la Privacidad de las Redes Globales pronunciada por la Organización para la Cooperación y el Desarrollo Económicos en el año 1998 tiene el objetivo de reafirmar el compromiso de este organismo sobre la protección de la privacidad de la redes globales para garantizar el respeto de importantes derechos, generar confianza en las redes globales y evitar restricciones innecesarias en los flujos transfronterizos de datos personales.

- El Marco de Privacidad fue acordado por los estados miembros del Foro de Cooperación Económica Asia Pacífico (APEC) en el año 2004, reconociéndose la importancia de la información en el desarrollo de negocios en la economía global y aspirando a la fluida circulación de información.

c. Tercera Etapa

Se trata de las referencias más modernas y actualizadas, donde se aprecia una concepción de la protección de datos como un derecho reconocido y completo, no solo con una faz económica, sino que social y cultural. Estas resoluciones, acuerdos y directrices buscan proteger el tratamiento de datos personales ante los peligros que genera el vertiginoso avance de las tecnologías de la información.

- Las Directrices para la Regulación de los Archivos de Datos Personales Informatizados, adoptadas mediante la resolución 45/95 de la Asamblea General de la Organización de las Naciones Unidas en el año 1990, consideran un catálogo de principios aplicables para el tratamiento de datos personales, siendo estos una garantía mínima que deben proporcionar los estados. El mismo documento establece su aplicación para las Organizaciones Internacionales Gubernamentales.
- Los Estándares Internacionales sobre Protección de Datos Personales y Privacidad pronunciados por la 31ª. Conferencia Internacional de Autoridades de Protección de Datos y Privacidad en el año 2009, es un documento marco que contempla una serie de principios, disposiciones generales y derechos para que los interesados puedan objetar el tratamiento de sus datos personales. Este texto marca una referencia en materia de protección de datos personales debido a su acabado desarrollo del tema.

Los Estándares Internacionales sobre Protección de Datos Personales y Privacidad, también conocidos como la *Resolución de Madrid*, es un texto elaborado por un grupo de autoridades de protección de datos de distintos estados, reunidos en la 31ª. Conferencia Internacional de Autoridades de Protección de Datos y Privacidad en el año 2009.

Destaca por su carácter consensuado y aporta una vocación universal de los principios y garantías que configuran este derecho. Además, reafirma la factibilidad de avanzar hacia un documento internacionalmente vinculante, que contribuya a una mayor protección de los derechos y libertades individuales en un mundo globalizado, y por ello, caracterizado por las transferencias internacionales de información.

Comienza con un apartado de disposiciones generales en que destaca los objetivos del documento y define ciertos términos, donde resaltan la incorporación de los conceptos de tratamiento, persona responsable y prestador de servicios de tratamiento. Se indica que el ámbito de aplicación es para el sector público y privado. También concede espacio para excepciones por motivos de la

seguridad nacional, la seguridad pública, la protección de la salud pública, o la protección de los derechos y las libertades propias de una sociedad democrática.

Posteriormente, continúa con un catálogo de principios básicos aplicables al tratamiento de datos personales, en el que se encuentran el principio de lealtad y legalidad, finalidad, proporcionalidad, calidad, responsabilidad y transparencia, imponiendo este último el deber de facilitar a los interesados información acerca de su identidad, de la finalidad para la que pretende realizar el tratamiento de los destinatarios a los que prevé ceder los datos de carácter personal y del modo en que los interesados podrán ejercer sus derechos.

En relación con lo anterior, establece un marco general de legitimación para el tratamiento de datos, es decir, bajo qué hipótesis un tercero puede tratar información. Contempla como hipótesis (i) Obtención del consentimiento libre, inequívoco e informado, (ii) Un interés legítimo del tercero, (iii) Cuando sea preciso para el mantenimiento o cumplimiento de una relación jurídica con el tercero, (iv) Aquellas ocasiones en que el tratamiento sea necesario para el cumplimiento de una obligación impuesta sobre el tercero por la ley y (v) Situaciones excepcionales que pongan en peligro la vida, la salud o la seguridad del titular de los datos u otra persona.

También considera un tratamiento especial a los datos sensibles, pues estima que deben tener una mayor garantía en su tratamiento. Sin embargo, no fija explícitamente estos mayores estándares, sino que lo deja a tarea de los estados.

Como novedad incorpora aquella situación en que el responsable del tratamiento le encomienda esta labor a un prestador de servicios de tratamientos, contemplando que ambos deben cumplir como mínimo con los estándares de protección de la Resolución de Madrid.

Al igual que otros documentos, se incorpora un punto respecto a los datos transfronterizos o transferencia internacional de datos, estableciendo como regla general que se podrán llevar a cabo, siempre cuando el estado receptor de los datos ofrezca como mínimo el nivel de protección contenido en la resolución ya mencionada.

Incorpora un acápite de derechos del titular de los datos, siendo estos el derecho de acceso, rectificación, cancelación y oposición (denominados derechos ARCO). Conjuntamente señala que el procedimiento para hacer efectivos dichos derechos debe ser sencillo, ágil y eficaz, y que no conlleven demoras o costes indebidos para el titular o interesado.

Este documento pone énfasis en la seguridad en el tratamiento de datos, primero al establecer que tanto el responsable como el prestador de servicios de tratamiento debe aplicar medidas técnicas y organizativas adecuadas. Se agrega la figura de la delación en aquellos casos en que se produzca una brecha de seguridad en el tratamiento de los datos; dicha denuncia busca que el interesado pueda evitar posibles afectaciones. Esto además se acompaña del deber de confidencialidad que recae sobre el responsable y todos aquellos que intervengan en el tratamiento.

Considera también las medidas que los propios estados puedan adoptar para una mejor y efectiva protección de datos, pues como se consigna en todo momento, el fin de estas recomendaciones no es oponerse a la circulación de datos, sino que estos fluyan con estándares mínimos de protección. Estas propuestas dicen relación con generar una cultura de protección de datos con políticas públicas claras y permanentes para que la sociedad valore su propia información.

Considera la existencia de un órgano de control o autoridad que vele por el cumplimiento de los principios y regulaciones. Dicho organismo debe cumplir ciertas características como ser independiente, imparcial, tener la suficiente cualificación técnica y poseer los recursos adecuados. Siendo esta entidad aquella en donde los interesados puedan efectuar sus reclamaciones, sin perjuicio de la vía jurisdiccional ya sea como vía alternativa o como control de sus decisiones.

- En el año 2013 la Organización para la Cooperación y el Desarrollo Económicos elaboró un documento denominado *Marco de Privacidad*, donde desarrolla la política del organismo en la materia y actualiza las directrices sobre protección de la privacidad elaboradas en el año 1980.

Este marco comprende la primera actualización de las Directrices sobre Protección de la Privacidad y Flujos Transfronterizos de Datos Personales del año 1980.

Como fundamento se esgrime el cambio tecnológico ocurrido en las tres décadas de vigencia del primer documento, lo que implica un desfase con la realidad y se traduce en un aumento en la cantidad de datos recolectados, tratados y almacenados, el análisis que se realiza a esos datos y las amenazas que esto genera a la privacidad.

En la primera parte se incorporan nuevas definiciones como *Leyes que protegen la privacidad* y *Autoridad de aplicación de privacidad*, siendo este último el reconocimiento de un organismo público que es responsable de la aplicación de las normas de protección de la privacidad.

En cuanto a los principios, estos se mantienen vigentes, solo incorporando conceptos como *rendición de cuentas* lo que significaría que los responsables del tratamiento de los datos adopten políticas para el cumplimiento real de la normativa de protección de datos, incorporando una sección especial sobre responsabilidad de ejecución.

También incluye el término de *notificación de las vulneraciones de seguridad* que consiste en un aviso a la autoridad y a los titulares de los datos sobre una falla de seguridad en el tratamiento de sus datos personales, lo que busca que las personas adopten los resguardos pertinentes.

Respecto a la transferencia internacional de datos, el documento toma en consideración nuevas técnicas de almacenamiento (como el *Cloud Computing*), pues responsabiliza al controlador de datos por el tratamiento de éstos, independientemente del lugar donde se encuentren almacenados los datos.

Por último, contempla el fomento de políticas públicas por parte de los estados, pues no se trata sólo de adoptar medidas legislativas, sino de impulsar también la cultura en materia de protección de datos y privacidad.

En esta fase también se encuentran los siguientes instrumentos:

- La resolución A/C.3/68/L.45/Rev.1 titulada *El derecho a la privacidad en la era digital,* fue aprobada por la Asamblea General de la Organización de las Naciones Unidas en el año 2013, en que se reafirma el deber de protección de la vida privada de las personas, esto a raíz del denominado Caso Snowden.
- La resolución AG/RES. 2842 de *Acceso a la información pública y protección de datos personales* aprobada por la Asamblea General de la Organización de los Estados Americanos en el año 2014, en donde se destaca la importancia de la protección de datos personales y el respeto al derecho a la privacidad.
- En el año 2015 se rinde cuenta ante la Asamblea General de la Organización de los Estados Americanos de un informe titulado *Privacidad y protección de datos personales*, elaborado por el Comité Jurídico Interamericano, indica los principios sobre la protección de la privacidad y los datos personales, los que deben guiar las legislaciones de los Estados Americanos en relación con el tema.

2. LEGISLACIÓN EXTRANJERA

Es posible encontrar múltiples legislaciones que regulen la protección de datos, sin embargo, se destacan los principales referentes: la Unión Europea, España y Uruguay. El primero, es relevante por su desarrollo en relación con la protección de datos personales y por la importancia atribuida a éstos. España destaca por ser uno de los estados con mayor nivel de garantías en la protección de datos, siendo un referente para Latinoamérica. Por último, Uruguay lo hace con una moderna regulación, inspirada en las legislaciones de Europa continental, lo que le ha valido ser reconocido como una nación con un nivel adecuado de protección de datos.

a. Unión Europea

La Comunidad Europea destaca por su compromiso por la adecuada protección de derechos, efectuada mediante los instrumentos jurídicos que dispone. Es por ello que la primera iniciativa formal que podemos encontrar es el denominado *Convenio 108* del año 1981.

Este documento tuvo por objeto el tratamiento automatizado de los datos personales, y a su vez fundó la protección de los datos en el respeto de las garantías fundamentales, además de agregar la categoría de datos sensibles y señalar los principios en esta materia que acompañan al derecho hasta el día de hoy.

No obstante, el instrumento jurídico que sentaría las bases en materia de protección de datos sería la *Directiva 46/95/C5*, del año 1995, que establece las bases de una mayor coordinación

entre las legislaciones nacionales, el cual aportó la obligación de cumplir un nivel adecuado de protección, agregando, además, normas de conflicto para dirimir pugnas interestatales, sistematizando los principios aportados por el *Convenio 108*, otorgando especial énfasis al principio de consentimiento.

Esta Directiva incorpora definiciones de *fichero de datos personales*, *encargado del tratamiento*, *tercero*, *destinatario* y de *consentimiento del interesado*. Contribuyendo a una mayor certeza al momento de observar el proceso de tratamiento de datos e incorporando nuevos términos que se hacían necesarios con la automatización en el tratamiento.

Agrega un régimen de excepciones a la aplicación del documento tales como la seguridad pública, la defensa, la seguridad del Estado y las actividades del Estado en materia penal. También los casos en que una persona física realice actividades exclusivamente personales o domésticas.

Establece un grupo de principios aplicables al tratamiento de datos, entre ellos: principio de legalidad, finalidad, calidad y seguridad. Regula las condiciones de legitimidad para el tratamiento de datos indicando la necesidad de un consentimiento inequívoco o en aquellos casos en que el tratamiento sea necesario para la ejecución de un contrato que involucre al interesado. También otorga una regulación especial a ciertos tipos de datos, principalmente los denominados datos sensibles.

Considera pertinente hacer mención a que los estados deben conciliar el derecho a la intimidad con el derecho a la libertad de expresión, y se deben establecer las excepciones razonables ante el tratamiento de datos personales con fines periodísticos, de expresión artística y literaria.

Y siguiendo en la dimensión de la protección efectiva de los datos, impone al responsable del tratamiento un deber de informar al titular de los datos cierta información básica como la identidad del responsable del tratamiento (o su representante), los fines con los que fueron recabados los datos, los destinatarios de los datos y dar cuenta de los derechos de acceso y rectificación.

Consolida el derecho de acceso, es decir, el derecho que tiene el interesado a saber si sus datos están siendo tratados, además de los fines y otros aspectos relevantes. En la directiva, respecto a este derecho se estipula que puede ejercerse sin restricciones, con una periodicidad razonable y sin retrasos ni gastos excesivos. Así, igualmente reconoce el derecho de oposición, según el cual todo interesado tiene la facultad de impedir que se realice el tratamiento de sus datos personales en todo momento y fundamentado en razones legítimas propias de su situación particular.

Un elemento singular es el reconocimiento que deben efectuar los estados, para que las personas tengan el derecho a no verse afectadas por una decisión con efectos jurídicos que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, entre otros elementos. Aunque lo anterior admite excepciones en aquellos casos en que se haya establecido en la celebración o ejecución de un contrato y cuando esté autorizado por ley.

En cuanto a la seguridad, la Directiva contempla un deber de confidencialidad tanto del responsable como del encargado de llevar a cabo el tratamiento e impone la obligación de adoptar todas las medidas técnicas y organizativas con el objetivo de garantizar la seguridad en el tratamiento.

En la misma línea de imponer deberes, le asigna al responsable (o al representante) de los datos el notificar a la autoridad de control cuando vaya a realizar el tratamiento de datos personales, siendo esta la regla general. Sin embargo, enumera una serie de excepciones o situaciones en que se permite una notificación simplificada.

Para asegurar el principio de seguridad se menciona que los estados deben configurar mecanismos de control previos al tratamiento de datos, para asegurar que dicho proceso sea realizado conforme a la legislación vigente y junto con lo anterior se debe llevar un registro de los tratamientos notificados, que puede ser consultado por cualquier persona.

En cuanto a las reclamaciones, se establece que los estados deben velar para que, independientemente de los recursos administrativos, exista un recurso judicial para garantizar la adecuada protección a los datos de las personas en casos de vulneración. También se deben establecer las cláusulas para hacer efectivo el principio de responsabilidad, además de señalar las respectivas sanciones.

Así mismo, pone énfasis en regular la transferencia internacional de datos personales (datos transfronterizos), permitiendo la dicha transferencia cuando el Estado receptor tenga un nivel adecuado de protección de datos y para calificar como tal, señala que el carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia. Se establecen criterios como la naturaleza de los datos, la finalidad y la duración del tratamiento, el país de destino final, las normas de Derecho vigentes en el país tercero que se trate y las medidas de seguridad en vigor en dichos países. Salvo excepciones que se contemplan en el documento como por ejemplo, previo consentimiento del interesado.

Una de las partes más relevantes de dicha Directiva es el establecimiento de una autoridad pública de control de la legislación vigente. A dicha autoridad, le atribuye una facultad consultiva en el momento de la elaboración de las medidas reglamentarias o administrativas relativas al tratamiento de datos de carácter personal. Así mismo, se le asignan atribuciones de investigación, poderes efectivos de intervención como formular dictámenes antes de realizar los tratamientos u ordenar el bloqueo, la supresión o la destrucción de datos, o incluso prohibir provisional o definitivamente un tratamiento. También debe presentar periódicamente un informe sobre sus actividades y publicarlo en conformidad a la legislación nacional.

El acto legislativo europeo crea en su artículo 29 un grupo de protección de las personas en lo relativo a la protección de datos, es por ello que al grupo se le denominó “grupo de trabajo del artículo 29”. Esta entidad estará compuesta por representantes de las autoridades de control de los estados miembros, un representante de la autoridad creada por los organismos comunitarios y

un representante de la Comisión. Este grupo tiene por cometidos velar por la aplicación homogénea de la directiva en los estados miembros, asesorar al Comité ante cualquier otra normativa que se plantee en materia de protección de datos y puede emitir recomendaciones por iniciativa propia en relación con su cometido.

Por último, hay que mencionar que desde el año 2012 se inició la tramitación de un Reglamento General de protección de datos, ante el Parlamento Europeo, el cual busca dar mayor solidez a los aspectos jurídicos que son relevantes en la materia. Así, la diferencia entre una Directiva como la actual y un reglamento, radica principalmente en que la primera es un acto legislativo en el cual se establecen objetivos, sin embargo, corresponde a cada Estado elaborar sus propias leyes sobre cómo alcanzar esos objetivos. Mientras que el segundo es un acto legislativo vinculante, es decir, deben aplicarse en su integridad en toda la Comunidad Europea.

Se puede destacar que se incorporan más términos que los contenidos en la Directiva actual, como *consentimiento del interesado*, *violación de datos personales*, *datos genéticos* y *datos biométricos,* en una clara muestra de añadir las nuevas tecnologías que se sustentan en datos personales.

Le otorga una mayor importancia al consentimiento al dar un apartado exclusivo a éste, incluso asignando la carga de la prueba al responsable del tratamiento de los datos. En la misma línea resguarda de forma especial el tratamiento de datos personales de los niños, debiendo ser los padres o tutores quienes autoricen un eventual tratamiento de sus datos.

Una de las principales novedades es la incorporación expresa del denominado derecho al olvido, el que está sujeto a ciertas hipótesis para su proceder, entre ellas la vulneración en aquellos casos en que los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos y cuando los datos hayan sido tratados ilícitamente.

Todas las autoridades públicas y las empresas que realizan determinadas operaciones de riesgo para la seguridad de los datos deberán nombrar un delegado de protección de datos. También señala la obligación para los estados miembros de crear una autoridad de control independiente a nivel nacional y pretende establecer mecanismos para lograr una aplicación coherente de la legislación sobre protección de datos en toda la Unión Europea. En particular, en los casos transfronterizos importantes en que estén implicadas varias autoridades nacionales de supervisión, se adoptará una única decisión de supervisión, es decir que una empresa con filiales en varios Estados miembros solo tendrá que tratar con la autoridad de protección de datos del Estado miembro de su establecimiento principal.

En los casos de infracciones dispone sanciones muy severas contra los responsables o encargados del tratamiento de datos. Los responsables del tratamiento podrían ser multados con hasta 20 millones de euros o el 4% de su volumen de negocios total anual. Las autoridades de protección de datos nacionales serán las que impongan estas sanciones administrativas.

b. España

La Constitución española del año 1978 consagra en su artículo 18.4 que la ley limitará el uso de la informática para garantizar la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos. Es de aquí que la doctrina constitucional desprende el derecho a la intimidad y a la protección de los datos personales, incorporándose así a un fenómeno cada día más común en las legislaciones modernas, esto es, la constitucionalización de la protección de datos personales.

En el año 1992 se promulga la *Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal*, también conocida como LORTAD.[1] Dicha normativa estuvo vigente hasta el año 1999 cuando se promulgó la Ley Orgánica de Protección de Datos de Carácter Personal. Dicho cambio normativo se fundamentó en que la primera ley no cumplía con los estándares mínimos exigidos por la Directiva Europea dictada en el año 1995, pues todos los estados debían adaptar sus legislaciones internas a dicha Directiva.

Hay que resaltar que la Ley del año 1999, vigente en la actualidad, ha sido una guía para las normativas latinoamericanas modernas, fundamentalmente por su visión garantista de la protección de datos personales, claramente influenciado por las referencias de la Unión Europea.

Dispone de una serie de conceptos y se reconocen un catálogo de principios aplicables a la protección de datos personales, entre los que destacan el de calidad, información en la recogida de datos, de consentimiento y de seguridad. A su vez también regula el tratamiento de ciertos datos de carácter sensibles y aquellos relativos a la salud de las personas.

Posteriormente se preocupa de las situaciones donde hay una transferencia de datos del responsable a un tercero, requiriéndose de un consentimiento para ello. Lo mismo ocurre en los casos en que el encargado de realizar el tratamiento sea un tercero distinto al responsable.

Consolida derechos de los interesados tales como la impugnación de valoraciones, el derecho a consultar el registro general, derecho de acceso, de cancelación, de rectificación y oposición, conjuntamente determina el procedimiento de reclamación para la tutela de estos derechos y fija el principio de responsabilidad.

Luego, la norma distingue entre una regulación sectorial entre las instituciones públicas y las privadas. Los ficheros o bases de datos públicas las regula en su creación, modificación y supresión, la comunicación o transferencia de datos entre las entidades públicas y sobre el tratamiento de datos en las fuerzas de seguridad. También establece un régimen de excepciones a los derechos que pueden ejercer los interesados.

Mientras que en el caso de los privados, regula su creación y establece un deber de notificación a la agencia de protección de datos informando de la conformación de una base de datos, a partir

[1] Cabe destacar que esta ley fue una de las normas que se tuvieron en cuenta al formular la ley N° 19.628 sobre protección de la vida privada en Chile.

de la cual se genera la inscripción en un registro general de bases de datos que lleva la misma autoridad. También genera un trato especial en ciertos ámbitos como en las áreas de solvencia patrimonial y crédito, de publicidad y de prospección comercial.

Determina la procedencia de la transferencia internacional de datos personales, indicando que por regla general no se permiten las transferencias a estados sin un nivel adecuado de protección de datos, calificación que depende de la agencia de protección de datos. Sin embargo, considera una serie de excepciones a la regla general antes descrita.

También regula orgánicamente la agencia de protección, definiéndola como ente de derecho público, con personalidad jurídica propia y plena capacidad. A su cargo estará un director, asesorado por un consejo consultivo, define las funciones que desempeñará dicha autoridad pública, además de reglamentar el registro general de protección de datos.

Luego contiene un apartado de infracciones y sanciones, las que están contenidas en un catálogo y son clasificadas como leves, graves y muy graves, pudiendo aplicarse multas que van desde los 900 a los 600.000 euros.

c. Uruguay

En la Constitución de la República Oriental del Uruguay, se encuentra en su artículo 72° lo que se puede denominar una cláusula abierta, es decir, se deja abierta la posibilidad de incorporar más derechos mediante este artículo. La ya mencionada carta fundamental señala *"La enumeración de derechos, deberes y garantías hecha por la Constitución, no excluye los otros que son inherentes a la personalidad humana o se derivan de la forma republicana de gobierno".*

Por su parte, en el año 2008 se promulgó la Ley Nº 18.331 sobre *Protección de datos personales y acción de habeas data*, la que en su primer artículo indica que el derecho a la protección de datos es un derecho inherente a la persona humana, por tanto se encuentra incorporado a la Constitución mediante el artículo 72 de dicho documento.

Dentro de las principales características de esta ley es que es moderna, garantista y además incorpora a las personas jurídicas como sujetos de protección, situación distinta a lo que ocurre en las legislaciones analizadas anteriormente y, en general, en el contexto internacional.

Las características antes descritas le han valido ser considerado un Estado con un nivel adecuado de protección de datos, lo que trae consigo la ventaja de ser receptor de datos por parte de los países de la Unión Europea sin mayores contratiempos ni permisos especiales. Esto le significa una ventaja en términos de competitividad económica, pues las empresas se valen de la calificación ya señalada para realizar los flujos transfronterizos de datos necesarios en la economía globalizada actual. Lo anterior le significó ser el primer país de Latinoamérica en ser invitado a adherir el denominado *Convenio 108* del Consejo de Europa, el que fue ratificado por la Ley N°19.030 de 2013.

La ley de protección de datos añade algunos conceptos, además de los habituales en este tipo de regulaciones, entre los que se encuentra el de "Disociación de datos" en que la información obtenida del tratamiento de datos no puede ser vinculada a una persona. Respecto a los principios que contiene, se encuentra el de legalidad, veracidad, finalidad, consentimiento informado, seguridad de los datos, reserva y responsabilidad.

Establece derechos como el de información frente al tratamiento de datos, es decir, el deber de informar al titular que sus datos fueron recolectados para ser tratados. También contempla el derecho de acceso, rectificación, actualización, inclusión, supresión y el derecho de impugnación de valoraciones personales.

Esta norma regula especialmente ciertos tipos de datos personales como los datos sensibles, los de la salud, de las telecomunicaciones, aquellos con fines publicitarios y con fines comerciales o crediticios.

En materia de datos transfronterizos establece una regla general que prohibe la entrega de datos a estados que no ofrezcan un nivel adecuado de protección de datos, sin embargo, establece una serie de excepciones como la cooperación judicial internacional o el consentimiento del interesado.

Regula de forma distinta las bases de datos públicas y las privadas, dotando a las primeras de excepciones al derecho de acceso, rectificación y cancelación. Mientras que para ambas existe un deber de ser incorporadas a un registro que lleva el órgano de control.

Igualmente crea un órgano o autoridad de control de datos personales, denominada Unidad Reguladora y de Control de Datos Personales. Se crea un consejo consultivo y se establecen las funciones que debe desempeñar este órgano, además de otros aspectos orgánicos.

Señala que la infracción de la norma conlleva una sanción que puede fluctuar desde una observación, apercibimiento, multa de hasta 500.000 unidades indexadas[2], la suspensión de la base de datos respectiva por el plazo de cinco días, hasta la clausura de la misma.

Como característica de esta regulación es que incorpora el procedimiento llamado *habeas data*, el que procedería bajo la hipótesis de una situación de error, falsedad, prohibición de tratamiento, discriminación o desactualización. Y esta acción judicial puede conducir a exigir su rectificación, inclusión, supresión o lo que entienda corresponder, respecto a los datos en cuestión.

[2] Según el Instituto Nacional de Estadística de La República Oriental del Uruguay, una unidad indexada es: *"Una unidad de valor que se va reajustando de acuerdo a la inflación medida por el Índice de Precios del Consumo. Esta unidad varía diariamente de modo que al cierre de mes acumula una variación con respecto al valor de la unidad indexada del mes anterior".*

CAPÍTULO II. MARCO NORMATIVO DE LA LEY N°19.628

La Ley N°19.628 sobre Protección de la Vida Privada, vigente en nuestro país desde agosto de 1999, tuvo origen en una moción presentada 6 años antes en el Senado. Se indicó que el proyecto de ley venía a llenar un vacío manifiesto en el ordenamiento jurídico y su propósito era dar una adecuada protección al derecho de la vida privada de las personas, ante eventuales intromisiones ilegítimas (Historia de la Ley, página 4).

En su tramitación en la Cámara de Diputados, el proyecto fue circunscrito a la normativa que regula el tratamiento de los datos personales por organismos públicos y privados, sin modificar la denominación de la Ley, no obstante contemplar un sólo un aspecto de la vida privada, *"cual es asegurar el derecho a la autodeterminación informativa, en lo referente al tratamiento de datos personales"* (Cerda, 2012: 14).

Si bien originalmente el proyecto estaba basado en leyes sobre informática y protección de datos de países como Francia, Gran Bretaña y Noruega, durante la tramitación posterior fue cobrando relevancia la Ley Orgánica 5/1992 sobre regulación del tratamiento automatizado de los datos de carácter personal (LORTAD) de España (Cerda, 2012: 14), ley que finalizó su vigencia a fines del año 1999, solo unos meses después de promulgada la norma chilena[3].

En este capítulo se examinan los principales aspectos de la Ley que fueron objeto de críticas por parte de implementadores y expertos entrevistados, principalmente en lo referido al ámbito de aplicación y también respecto a las definiciones normativas, es decir, aquellos conceptos que entrega la misma norma y que se presentan como elementos claves al momento de su aplicación.

Asimismo, se analiza la visión plasmada en la Ley sobre legitimidad del tratamiento de datos personales, con un especial enfoque en la regulación del consentimiento y el amplio estatuto de excepción a esta figura.

Finalmente, el procedimiento de amparo a los derechos consagrados y las sanciones establecidas en la Ley fueron también objeto de observaciones por parte de los entrevistados, en particular debido a la importancia en el cumplimiento efectivo de la norma y del objetivo de protección impuesto por el Legislador.

[3] Dicha Ley fue derogada expresamente por la Ley Orgánica 15/1999, de Protección de Datos de carácter Personal. Sitio web de la Agencia Española de Protección de Datos.
http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/common/pdfs/2014/Ley_Organica_15-1999_de_13_de_diciembre_de_Proteccion_de_Datos_Consolidado.pdf

1. PRINCIPIOS DE LA LEY N° 19.628 SOBRE PROTECCIÓN DE LA VIDA PRIVADA

Es común encontrar en la normativa relativa a la protección de datos personales un catálogo de principios que inspiran y conducen la interpretación de la propia legislación. En algunas ocasiones se encuentran en un capítulo específico, otras en cambio se hallan dispersas en la misma norma.

a) Principio de Libertad en el Tratamiento

Contrariamente a lo que muchas personas pueden pensar, el establecer una normativa que regule el tratamiento de datos personales no busca prohibir que se realice el tratamiento de datos personales, pero sí que este se lleve a cabo conforme a la normativa.

Dicha libertad de tratamiento la podemos encontrar en el artículo 1° de la ley referida, al señalar que "*Toda persona puede efectuar el tratamiento de datos personales*". Por tanto, podemos considerar esta libertad como la regla general, pero a su vez se establecen ciertas restricciones a este principio.

Primero, que el tratamiento de datos personales debe efectuarse en conformidad a la presente normativa. Segundo, que la finalidad de dicho tratamiento debe obedecer el ordenamiento jurídico. Tercero, que se deberá respetar el pleno ejercicio de los derechos fundamentales de los titulares de los datos y de las facultades que esta ley les reconoce. En consecuencia, encontramos el principio de libertad en el tratamiento, sujeto a tres atenuaciones que la propia norma contempla expresamente.

b) Principio de Licitud

Este principio se encuentra relacionado con el anterior, pues la libertad de tratamiento se encuentra a su vez limitada por el principio de licitud, según el cual solo se pueden tratar datos cuando exista una autorización legal, ya sea de la propia Ley N°19.628 u otra norma.
Este principio se encuentra consagrado en el artículo 4° de la citada ley, al señalar que *"El tratamiento de los datos personales sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen".*

c) Principio de Información y Consentimiento

El principio de información pretende que el titular de los datos personales tome conocimiento de la recolección de sus datos, el propósito o finalidad del tratamiento y sobre la posibilidad de comunicarlos al público. Al menos así lo contempla nuestra norma en su artículo 4° indicando que *"La persona que autoriza debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público".*
Establecer este principio es de toda lógica, pues si el titular de los datos no conoce que sus datos están siendo tratados difícilmente podría ejercer los derechos que contempla la misma normativa, o bien, al menos poder ejercer una labor de vigilancia o fiscalización del tratamiento.

Además, el informar se relaciona con el consentimiento. Esta regulación contempla un consentimiento previo, libre e informado. El mismo artículo antes citado señala que el tratamiento se puede efectuar cuando una disposición legal lo permita o el titular de los datos lo autorice expresamente.

Con respecto a esto último, contempla que la autorización debe ser escrita y es susceptible de ser revocada, pero sin efecto retroactivo, es decir, que el tratamiento ya efectuado es legítimo e igualmente la revocación debe constar por escrito.

A su vez, este consentimiento, que es la llave para acceder al tratamiento de datos, posee ciertas excepciones como los datos que provienen de fuentes accesibles al público, el tratamiento de datos realizado por personas jurídicas privadas para sus fines y usos exclusivos y aquel efectuado por organismos públicos.

Sin embargo, como indica el abogado especialista en Derecho y Tecnología Alberto Cerda, se extraña una disposición que obligue al responsable del tratamiento a informar al titular de los datos que estos van a ser tratados y la fuente de donde se obtuvieron.

d) Principio de Finalidad

Como se señaló anteriormente, la finalidad es una de los aspectos que deben ser informados al momento de obtener el consentimiento. Este principio busca proteger el propósito para el cual fueron recogidos los datos personales, haciéndolo extensivo a su tratamiento.

Así entonces, si el responsable recoge datos con la finalidad de otorgar un beneficio a sus clientes, esos datos no pueden ser utilizados para otro fin, salvo que el titular consienta en ello.

En el artículo 9° de la norma en comento se establece este principio y la excepción en aquellos casos en que los datos provengan de una fuente accesible al público, esto debido a que al ser una fuente de acceso público, está exento de consentimiento y su obtención no estuvo sujeta a una finalidad determinada.

En el año 2012 se promulgó la Ley N° 20.575 que buscó regular el principio de finalidad en el tratamiento de datos personales de carácter económico, financiero, bancario y comercial. La norma determinó que estos datos solo pueden ser transferidos al comercio establecido para fines de una evaluación de riesgo comercial o en el marco de un proceso crediticio. Excluyendo su uso para otros fines como selección de empleos, admisión académica, atención médica, entre otros.

e) Principio de Calidad de los Datos

Lo encontramos en el artículo 9° de la Ley N°19.628 e indica que los datos deben ser exactos, actuales y reflejar con veracidad la realidad del titular de los datos. También estos datos deben ser adecuados y no excesivos en relación con los fines que se persiguen con su tratamiento.

Por tanto, como señala el académico Alberto Cerda (2012) este principio se compone de dos ideas: los datos deben reflejar verazmente la realidad y ser adecuados, pertinentes y no excesivos en relación con el fin que fueron recogidos. Incorporándose así un criterio de proporcionalidad que forme parte del principio de calidad.

f) Principio de Seguridad

La legislación no solo busca proteger el adecuado tratamiento de datos personales mediante los derechos que les otorga a los titulares de los datos, sino también impone ciertos deberes a aquel que se configura como el responsable del tratamiento. Este principio de seguridad impone al responsable el deber de adoptar todas las medidas técnicas, de seguridad y organizativas que sean necesarias para el tratamiento con estándares de confidencialidad y buen manejo de datos.

En el artículo 11° de la Ley N°19.628 se contempla el deber de debida diligencia que recae sobre el responsable del tratamiento, haciendo responsable incluso de los eventuales perjuicios que pudiesen afectar a los titulares. Sin embargo, no se contempla de forma más clara bajo qué criterios determinar la debida diligencia en el ámbito del tratamiento de datos personales. De esa forma son los tribunales de justicia quienes deben establecer los parámetros y además aplicarlos.

De este mismo artículo también se puede extraer el principio de responsabilidad, es decir que aquel que trata los datos debe hacerse responsable de los posibles perjuicios que le traiga al titular el tratamiento inadecuado de sus datos personales.

g) Deber de Secreto

Relacionado con el principio anterior, este secreto corresponde a un deber que recae sobre todos aquellos que intervinieron en el tratamiento de datos personales y que implica garantizar estándares de confidencialidad y reserva de la información.

En la norma actual podemos reconocerlo en el artículo 7°, indicando que esta norma afecta a las personas que trabajan en el tratamiento de datos personales, indistintamente de si se trata del mundo privado o público, siempre que correspondan a datos que no hayan sido obtenidos de una fuente accesible al público. Además establece que este deber de reserva perdura más allá del período en que se efectúe el tratamiento mismo, aunque sin especificar el límite temporal.

2. ÁMBITO DE APLICACIÓN DE LA LEY N°19.628

Tal como lo señala su artículo primero, la Ley N°19.628 regula el tratamiento de los datos de carácter personal, tanto por organismos públicos, privados y por particulares, a excepción del que se efectúe en ejercicio de las libertades de emitir opinión e informar.

La Ley permite el tratamiento de datos personales siempre que se haga de manera concordante con ésta y para finalidades permitidas por el ordenamiento jurídico. Asimismo, consagra el respeto al pleno ejercicio de los derechos fundamentales de los titulares de los datos y a las facultades que la norma les reconoce.

Respecto a la excepción señalada en el artículo primero, la regulación que prima sobre la libertad de opinar e informar es aquella del artículo 19 N° 12 de la Constitución Política y actualmente, la de la Ley N°19.733, sobre Libertades de Opinión e Información y Ejercicio del Periodismo. En ambas se califica dicha libertad, sin censura previa, como derecho fundamental, sin perjuicio de responder de los delitos y abusos que se cometan en el ejercicio de estas libertades.

Para la Fundación Datos Protegidos, la libertad para efectuar tratamiento de datos como principio básico consagrado en la Ley, es calificado como positivo, sin embargo, debe ir acompañado de la posibilidad de control por parte del titular y por ende, de una regulación que lo proteja.

"Las leyes de tratamiento de datos personales lo que no tienen que hacer es limitar el libre flujo de la información. No se trata de esconder, no se trata de privacidad, de confidencialidad, sino que se trata de regular el tratamiento. Es decir, desde que un dato se almacena, cuánto tiempo, quién lo va a ver, las medidas de seguridad, cuál es la finalidad, si es exacto, veraz, si es actualizado".

Respecto de los organismos públicos, la Ley los define de una manera amplia, incluyendo las autoridades, órganos del Estado y organismos regulados por la Constitución, como por ejemplo, Congreso Nacional, Poder Judicial, Contraloría, entre otros. Asimismo, incorpora también los comprendidos en la Ley N° 18.575, bajo el concepto de Administración del Estado. Estos últimos reúnen a los Ministerios, Intendencias, Gobernaciones, Municipalidades y empresas públicas creadas por ley, entre otros.

"Es más amplia que la Ley de Trasparencia que tiene un régimen especial para el Poder Judicial, para el Poder Legislativo, para la Contraloría, y hay una ley que aplica a los servicios públicos en general. En cambio esta Ley, aplica para los órganos de la administración, para los órganos del Estado en general". (Fundación Datos Protegidos)

Por otra parte, con relación a los particulares, desde el Centro de Estudios en Derecho Informático de la Universidad de Chile dieron cuenta de la falta de pronunciamiento de la Ley sobre este

concepto. Lo anterior, indicando que no existe claridad si se incluye a personas naturales solamente o también a personas jurídicas.

"Por ser un tema que tiene que ver con un derecho constitucional tiene que ver con las personas naturales solamente, pero sí logro entender por qué efectivamente ciertas normas podrían imponerse a las personas jurídicas".

Por otra parte, el Comité de Retail Financiero, en documento entregado para la investigación, puso énfasis en la necesidad de perfeccionar el ámbito de aplicación de la ley en especial desde un punto de vista territorial. Así, expresaron que la prestación de servicios globales fuera de Chile debe asegurar el pleno respeto de la nueva legislación, no pudiendo bastar el hecho que el responsable del tratamiento de datos no se encuentre en el país para que no se le haga aplicable la misma.

También algunos plantearon la necesidad de definir si la Ley regula todo tipo de bases de datos, o sólo aquellas que tengan ciertas características que la hagan relevante para este efecto. En ese sentido se pronunciaron desde el Centro de Estudios en Derecho Informático (CEDI) y el ex asesor del Ministerio de Economía, Raúl Arrieta.

"No puede ser que esta ley como está hoy día se le aplique a la libreta de teléfonos de mi abuelita... es absurdo." (Raúl Arrieta)

Al respecto, cabe señalar que el anteproyecto de la Presidenta Bachelet que se sometió a consulta en el año 2014, excluía de su aplicación a aquellas bases de datos domésticas. Sin embargo, no existe claridad si el proyecto trabajado por el Ejecutivo en 2016 contendrá la misma norma siguiente:

"El régimen de protección de datos personales que se establece en esta ley no será de aplicación a las bases de datos mantenidas en un ambiente exclusivamente personal o doméstico y para actividades relacionadas con su vida privada y familiar. En caso que pierdan tal carácter quedarán sujetas a las disposiciones contenidas en esta ley".

Con respecto a la denominación de la Ley N° 19.628, como "Sobre protección de la vida privada", algunos expertos manifestaron su discrepancia. En este sentido, fue notado que los datos personales pueden tener un carácter público o privado, pero manteniendo la calificación de personales. Esto puede observarse especialmente respecto a datos sensibles como la afiliación sindical, el cual no es un dato privado, no afecta la vida privada, pero sí es un dato personal sensible porque puede dar lugar a discriminación.

"La ley se había dictado en una primera época, donde todo el mundo estaba confundido y pensaba que esto tenía que ver con la privacidad. Hoy en día, el mundo civilizado se dio cuenta, que esta cuestión no tiene que ver con la privacidad. Hay un ámbito de la ley que se refiere a la privacidad,

pero un pedacito que se refiere a la privacidad. Existe un gran espacio, donde son datos públicos que si son mal manejados, terminan en abusos o decisiones arbitrarias respecto de las personas". (Lorena Donoso, Presidenta Instituto Chileno de Derecho y Tecnología)

En este sentido la experta estimó, que el objetivo de la Ley debiera ser proteger a las personas respecto del tratamiento de sus datos, sean privados o públicos, porque un tratamiento abusivo de estos datos, aunque sean públicos, puede dar pie a discriminaciones arbitrarias.

3. CONCEPTOS PRESENTES EN LA LEY N°19.628

Siguiendo la tendencia comparada sobre la materia, la Ley en su artículo 2° enumera y define una serie de conceptos o definiciones legales. Entre ellos podemos encontrar los siguientes:

a) Dato estadístico y dato personal

- Dato estadístico: el dato que, en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable.
- Datos de carácter personal o datos personales: los relativos a cualquier información concerniente a personas naturales, identificadas o identificables.

Respecto a lo anterior, algunos entrevistados manifestaron la necesidad de mejorar la definición de datos personales, argumentando la falta de elementos que permitan establecer cuándo un dato es personal o no. En este sentido, algunos señalaron la discusión no resuelta respecto a ciertos datos como la patente de un vehículo, la dirección IP, entre otros, que la conceptualización actual legal no permite resolver.

"El número del celular ¿es un dato personal? ¿El Rut es un dato personal? ¿La dirección es un dato personal? Entonces, en Chile todavía estamos en esa discusión que es súper básica, o sea, muchas personas dicen que el RUT no es un dato personal porque es público, pero no, los datos personales pueden ser públicos o pueden ser privados". (Fundación Datos Protegidos)

Asimismo, se refirieron a la problemática de dotar de contenido al concepto de "persona identificable", en especial en consideración a los medios que se pueden emplear para identificar a una persona, considerando la tecnología actual.

"¿Qué es persona identificable? ¿Qué medios tengo? Cualquier persona es identificable. Si estoy en un estadio y pasa una cámara todas esas personas, dependiendo de la resolución de la cámara, son identificables en la medida que pueda hacer el circuito del rostro. ¿Entonces a todas esas personas para grabarlas tengo que pedirles el consentimiento?" (Consejo para la Transparencia)

Al respecto, el académico Alberto Cerda sostiene que la ley pretende extender la protección al tratamiento de aquellos datos que conciernen a toda persona cuya identidad puede llegar a ser establecida, y en este sentido cita la Directiva 95/46/CE, que considera "*el conjunto de medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona*" (Cerda, 2012: 16).

Por otro lado, se criticó también la falta de límite certero entre los conceptos de "dato personal" y "dato estadístico", calificando de insuficiente las nociones entregadas por la Ley y señalando la relevancia de contar con definiciones actualizadas que constituyen la base de la protección que se pretende otorgar.

"¿Cuando se transforma en dato estadístico? ¿Basta con que le borre el nombre o el rut a la persona? Eso no me lo resuelve la definición de dato personal, la definición está muy desfasada de la realidad". (Consejo para la Transparencia)

b) Datos sensibles

La Ley en la letra g) del artículo 2° define datos sensibles como "*aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad*".

A continuación, ejemplifica de modo no taxativo, ciertos datos de carácter sensible:

- Hábitos personales
- Origen racial
- Ideologías y opiniones políticas
- Creencias o convicciones religiosas
- Estados de salud físicos o psíquicos
- Vida sexual

Respecto a esta materia, la Organización Derechos Digitales calificó como positiva la definición actual debido a su amplitud y a su carácter abierto. Sin embargo, criticó la falta de un mayor número de ejemplos, respecto de los cuales se pudiera señalar que indudablemente son datos sensibles.

"Por ejemplo, nosotros no sabemos si la configuración facial es un dato sensible o no. Nosotros lo vimos en el caso del uso de los globos, donde nosotros tratamos de argumentar de que los rasgos biométricos, son información sensible. También existe duda si el Rut es información sensible."

Por su parte, el Consejo para la Transparencia señaló la necesidad de perfeccionar el concepto de datos sensibles. En ese sentido, dieron cuenta de experiencias a nivel comparado en que la definición está dada por la posibilidad de eventuales discriminaciones en base a esos datos. A

modo de ejemplo, señalan el caso de la afiliación política que es claramente un dato sensible, sin embargo, una norma amplia que incluya fuentes eventuales de discriminación permitiría incorporar también cualquier tipo de vinculación política u otros hechos para ser calificados como sensibles.

"Las definiciones a nivel internacional de datos sensibles junto con tratar de dar muchos ejemplos, tratan de precisar en esa lógica o ese concepto abierto de dato sensible, puesto que el dato sensible efectivamente no es solo aquellos que están mencionados ahí, mis creencias religiosas, afiliación política, hay otros muchos que podrían ser datos sensibles".

En el mismo sentido se pronunció la Organización Derechos Digitales, indicando la necesidad que la definición legal fuera abierta y no contuviera todos los tipos de datos sensibles de forma cerrada, sino un catálogo ejemplar.

"Usualmente las legislaciones del mundo, dan una lista ejemplar de información sensible que se refiere o que suele referirse a esferas de la intimidad, a pesar que parte de esa información no es necesariamente íntima, pero sí es información que uno prefiere no revelar en ciertos contextos. Por ejemplo, la afiliación política o la orientación sexual, que es una cuestión muy contextual".

Al respecto, de forma similar se pronunció el abogado especialista Carlos Reusser, quien señaló la importancia de mantener una definición amplia y de carácter abierto. *"Porque en realidad un dato sensible, es cualquier información que por sí misma puede dar pauta a que se produzca una discriminación a las personas".*

Particularmente, se señaló por el Consejo la conveniencia que la definición legal contenga no solamente la descripción de cuáles serían los datos, sino también elementos que permitan caracterizar el dato, de tal manera de contar con herramientas suficientes para poder encasillar en la definición cualquier situación que pueda generarse en el futuro. Al respecto, se hizo presente la debilidad actual de la Ley referente al catálogo de principios.

"La ley tampoco te da las herramientas como para interpretarla porque tampoco tiene un catálogo de principios diseñado, que te permita abrir la puerta para que frente a una definición o concepto determinado tú en base a los principios puedas darle salida para encajar en la situación que te vayas a encontrar más adelante".

Asimismo, el Consejo, en documento aportado a la investigación, abogó por una protección especial a los datos sensibles y una regulación pormenorizada de aquellos relativos a la salud, los biométricos, de identidad genética o biomédica, el origen racial, la vida y la orientación sexual, afiliación, ideología u opinión política, las creencias o convicciones religiosas o los datos relativos a niños, niñas y adolescentes.

En particular respecto a la regulación de los datos sensibles, Derechos Digitales hizo hincapié en la necesidad que se acompañe de términos más estrictos. Es decir, que el estándar de consentimiento sea más alto, expreso en vez de tácito, que se incorporen obligaciones especiales de información, conservación, seguridad y revisión de comunicación a terceros. O bien, una obligación especial de registro de base de datos que incluyan datos sensibles de personas, con las sanciones asociadas por el no registro de esas bases de datos o por no comunicar que son bases que tienen datos sensibles.

"Desde el punto de vista operativo, es especialmente relevante establecer mecanismos de observancia de esa clase de datos". (ONG Derechos Digitales)

Asimismo, se señaló la fuerte conveniencia de establecer sanciones más gravosas frente a infracciones a los deberes establecidos respecto de un dato sensible, por la especial naturaleza del dato que se trata.

Específicamente respecto a los datos de menores de edad, el Consejo para la Transparencia enfatizó la necesidad que se regulen y califiquen como datos sensibles, de manera de otorgarle una especial protección que actualmente no existe.

"El Consejo para la Transparencia, a pesar de que el artículo que define los datos sensibles no contempla los datos de menores como dato sensible, ha hecho una construcción en base a la Convención Internacional de Derechos del Niño y ha elevado a categoría de datos sensibles los datos de los niños y adolescentes. Es un esfuerzo interpretativo."

Sin embargo, cabe tener presente que la interpretación del Consejo para la Transparencia tiene aplicación efectiva sólo respecto de la facultad que dicho organismo tiene de velar por el cumplimiento de la Ley por parte de los Órganos de la Administración del Estado, de conformidad a la letra m) del artículo 33 de la Ley N°20.285, y por ende no se aplica al sector privado.

c) Fuentes accesibles al público

La letra i) del artículo 2° define "fuentes accesibles al público" como "*los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes*".

Respecto a este concepto, el Centro de Estudios de Derecho Informático de la Universidad de Chile, declaró no existir hoy una definición correcta de fuente de acceso público y señaló que, en la actualidad, todo aquello que no sea reservado o confidencial pasa a ser una fuente de acceso público.

"Internet, por ejemplo, hoy día podría ser una fuente de acceso público y en el extremo yo podría decir que si me encuentro con una serie de datos personales en internet, yo no debiera solicitar el

consentimiento del titular ni debiera requerir de una ley y podría perfectamente disponer, tratar o procesar [esos datos]".

En el mismo sentido se pronuncia el académico Alberto Cerda, al calificar el concepto como particularmente ambiguo, "*ya que no precisa si para la calificación de una fuente como accesible al público debe atenderse a circunstancias de hecho, o bien si ello supone la concurrencia de una habilitación normativa"*. En el primer caso, toda fuente podría ser de público acceso, salvo disposición legal en contrario, mientras que en el segundo, serían fuentes sólo aquellas que por expresa disposición legal revistan tal carácter. Esta última interpretación se avendría de mejor manera con el espíritu de la Ley y el carácter excepcional de la figura (Cerda, 2012: p. 21).

Por su parte, el Consejo para la Transparencia, en documento aportado para la presente investigación, criticó el concepto de fuente accesible al público por cuanto radica en el titular del registro o banco de datos "*la facultad de dejar o no abierto al público un registro, con el consecuente riesgo cierto de fraude al espíritu de la ley, especialmente, en lo que dice relación con la posibilidad de realizar tratamiento de datos sin autorización del titular*".

d) Responsable del registro o banco de datos

El concepto de responsable del registro o banco de datos se encuentra definido por la letra n) del artículo 2° y consiste en "*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*".

Respecto a esta materia algunos expertos señalaron el vacío legal que existe actualmente respecto a la distinción entre los diversos actores que intervienen en los procesos de tratamiento de datos personales. En particular, Nicolás Yuraszeck, enfatizó la importancia de distinguir específicamente entre los conceptos de responsable, como aquella persona que toma decisiones en base a una autoridad sea en un organismo público o empresa, y procesador, es decir, aquella persona que realiza por orden de un tercero este tratamiento de datos.

"En el derecho comparado, esto va a traer consecuencias en lo que significa la responsabilidad sobre el tratamiento de datos. No podemos esperar que una persona que tiene la decisión sobre el tratamiento de datos personales, tenga el mismo nivel de responsabilidad que con respecto a la persona que los procesa". (Nicolás Yuraszeck)

Ahondando en lo anterior, señala Yuraszeck que en el derecho comparado se habla de intermediarios, haciendo hincapié en la importancia de distinguir entre aquella persona que realiza un tratamiento de datos personales y aquellos intermediarios, como por ejemplo, un motor de búsqueda.

"Debemos recordar que hay buscadores que por ejemplo, solamente indexan datos. Ellos indexan el contenido o indexan el dato de distintas personas. Ellos no realizan propiamente tal un tratamiento de datos personales. Y esto tenemos que hacerlo asimilable".

En un mismo sentido se pronunciaron desde el Centro de Estudios de Derecho Informático (CEDI), señalando la importancia de distinguir correctamente entre el titular de un dato personal, el controlador y el procesador. En particular, señalaron que el titular de los datos es dueño de ese dato personal; mientras que el controlador del dato es quien los recibe de manera directa, no adquiriendo la titularidad ni la propiedad del dato, sino la mera tenencia. Este controlador puede procesarlos y tratarlos o puede contratar a un intermediario que da el servicio de procesamiento. Este último, es el procesador de los datos.

"La ley actual no hace correcta distinción en cuáles son los roles y las responsabilidades que tiene el controlador y el procesador del dato, y esto sí lo hacen otras legislaciones del mundo (…). Esa diferenciación, ese estatuto jurídico que debiera ser distinto hoy día no es tal. No está bien reconocido y habría que hacer los ajustes pertinentes".

Por su parte, el Consejo para la Transparencia, en documento aportado a la investigación, señaló que la ley, si bien define al responsable del registro o banco de datos, no se hace cargo de definir al responsable del tratamiento de los datos, que es la persona que toma las decisiones operativas respecto del banco de datos y en quien debiera radicar la responsabilidad directa por el uso indebido de los datos personales.

En sentido similar se pronunciaron desde la ONG Derechos Digitales, al dar cuenta del vacío legal respecto a los deberes, obligaciones concretas del encargado del tratamiento de datos. En efecto, señalaron que no existen hoy en día parámetros objetivos ni específicos respecto a la responsabilidad del encargado de bases de datos.

4. REGULACIÓN DEL CONSENTIMIENTO

El artículo 4° de la Ley N° 19.628 permite el tratamiento de los datos personales y lo considera lícito únicamente en las siguientes situaciones:

- Cuando dicha ley u otras disposiciones legales lo autoricen
- Cuando el titular consienta expresamente en ello.

De este modo, no existiendo norma legal que exima del consentimiento, la legitimidad del tratamiento de datos está condicionada a la autorización del titular de los datos.

Para el especialista Raúl Arrieta, el contenido esencial del derecho de la protección de datos se configura a partir de la legitimidad del tratamiento de estos, y la necesidad de legitimidad en el tratamiento de datos no admite excepciones. Esta legitimidad viene dada, en estricto rigor, por el consentimiento del titular, existiendo algunos casos en los cuales la Ley suple la voluntad del titular por considerar que hay otros intereses en juego que serían más relevantes.

Por otra parte, el especialista señala que existen casos en los cuales está implícita la necesidad de tratamiento de datos sin la obtención de autorizaciones específicas, como por ejemplo, en un contrato de trabajo, aunque no se dé la autorización de tratar la información previsional de la persona, ésta debe ser tratada en orden a poder pagar las cotizaciones previsionales. Sin embargo, estos casos no son reconocidos por la Ley, por lo que el régimen de excepciones actual estaría incompleto.

En un sentido similar se pronunciaron desde la Cámara Chilena Norteamericana de Comercio[4], al señalar como indispensable la incorporación de una serie de excepciones en la normativa, algunas señaladas en el Anteproyecto sometido a consulta ciudadana, en particular:

- El uso doméstico: para el ejercicio de actividades personales o domésticas.
- Las relaciones contractuales y precontractuales: cuando el tratamiento es necesario para la ejecución de un contrato en que el titular es parte o para la aplicación de medidas precontractuales.
- Cumplimiento de obligación legal o jurídica: cuando el tratamiento es necesario para el cumplimiento de una obligación del responsable.
- Para la protección de intereses vitales del titular u otra persona.

En cuanto al consentimiento, el artículo citado señala que la persona que lo otorga debe ser "*debidamente informada respecto del propósito del almacenamiento de sus datos personales y su*

[4] En documento elaborado especialmente para la investigación.

posible comunicación al público". Asimismo, dispone que esta autorización debe constar por escrito.

Al respecto, el especialista en derecho informático Carlos Reusser manifestó que la tendencia actual no se orienta hacia una escrituración necesaria del consentimiento, sino más bien a asegurar que sea inequívoco. En el mismo sentido se pronunció el abogado Raúl Arrieta.

"El consentimiento inequívoco lo que hace es trasladar la carga de la prueba a quien trata los datos personales, en el sentido de que si quien realiza la operación de tratamiento de datos personales no logra acreditar que obtuvo el consentimiento inequívoco del titular de los datos, esa persona carece de legitimidad para realizar la operación de tratamiento de datos".

Además de lo anterior, Arrieta pone énfasis en el deber y responsabilidad de quien realiza la operación de tratamiento de datos de establecer los mecanismos técnicos que permitan a los titulares de datos dar un consentimiento inequívoco y suficientemente informado.

Por su parte, desde el Centro de Estudios de Derecho Informático de la Universidad de Chile manifestaron la poca conveniencia de la definición actual, es decir el estándar de consentimiento general y obligatorio respecto de todos los tipos de datos posibles. Asimismo, sostuvieron la necesidad de regular el consentimiento de una forma más flexible asegurando una mejor adaptación a la realidad.

"Debiera haber distinción para el tipo de consentimiento que se pida tomando en cuenta el tipo de dato que se trata. Me parece que hay datos sensibles que evidentemente requieren de un consentimiento expreso previo porque van a ser datos que en cualquier contexto en que se usen requieren de una protección robusta, pero hay otros datos en que perfectamente sería posible pensar en un consentimiento inequívoco y que no necesariamente tenga que ser previo".

Desde el Consejo para la Transparencia dieron cuenta de las dificultades para determinar cuándo el consentimiento consta por escrito, esto con relación a la utilización de tecnologías informáticas en su otorgamiento. Asimismo, notaron las complejidades para acreditar que la persona detrás del computador es quien efectivamente debe dar o dio el consentimiento.

5. ESTATUTOS DE EXCEPCIÓN

La Ley N°19.628 permite el tratamiento de datos personales sin requerir el consentimiento de su titular en una serie de situaciones, la mayoría contenidas en el artículo 4° y otras dos en el artículo 10° y 20°.

Respecto a lo anterior, el académico Alberto Cerda señala que el legislador ha considerado que en determinadas circunstancias resulta imposible o difícil conseguir el consentimiento, o que puede legítimamente prescindirse de este en atención a la naturaleza de la fuente de la cual ha sido tomada la información o de los intereses estimados prevalentes (Cerda, 2012: 21).

De este modo, se configuran las excepciones a la regla de requerir el consentimiento en la Ley N°19.628. Estas normas fueron criticadas por los expertos e implementadores entrevistados, debido a su amplitud, lo que dejaría el principio del consentimiento con poca utilización y convertirían este principio general en la excepción.

"Primero con el principio general del consentimiento, pero luego viene una serie de excepciones, que prácticamente, cualquier tratamiento cae en esa excepción. Entonces esta es como la norma bolsillo de payaso, donde puedes sacar cualquier cosa". (Fundación Datos Protegidos)

a) Fuentes accesibles al público

La principal crítica está orientada hacia la noción de fuentes accesibles al público. Este concepto permite el tratamiento de ciertos datos por cualquier persona sin contar con la autorización o consentimiento del titular, siempre que el dato haya sido obtenido de una fuente accesible al público.

"Pero esta noción de fuente accesible al público, lo que hace es convertir, para todos los efectos prácticos, la regla general de solicitar autorización de titulares en la excepción". (Organización Derechos Digitales).

En este caso, fue comentada la oportunidad en que la base de datos del Servicio Electoral estuvo disponible en su totalidad en línea, por lo que para todos los efectos jurídicos todo lo contenido en dicha base es fuente accesible al público y por tanto puede ser tratada sin autorización de los titulares, aunque en la actualidad ya no esté disponible. Asimismo, se incluye también aquellas fuentes en que se debe pagar por acceder a ellas.

"Eso significa que cualquier base de datos que sea como fuente accesible al público, que no necesariamente tiene que ser público, es decir, accesible por cualquiera, pero si por ejemplo que tu tengas que pagar para acceder a ella, como la base de datos del boletín comercial por ejemplo, si eso lo sumas a que no tienes que inscribir las bases de datos, tienes el hecho de que cualquier dato

que esté en este tipo de fuentes, como que vuela, tú la agarras y después le perdiste el rastro". (Organización Derechos Digitales)

Con relación a lo anterior, la Organización plantea el problema de la fidelidad y actualización de la información contenida en dichas fuentes. En este sentido, señalan que al no ser obligatorio la inscripción de las bases de datos, no existe forma de saber cuántas personas están tratando dichos datos obtenidos a partir de una fuente accesible al público, y por tanto no hay forma de controlar y asegurar que dicho dato esté actualizado y sea fidedigno. De este modo, indican que puede ocurrir que al momento de la obtención del dato éste haya estado actualizado, pero luego de su tratamiento e incorporación en otra base de datos se encuentre caduco.

Desde el Centro de Estudios de Derecho Informático (CEDI) se pronuncian también criticando los estatutos de excepción al consentimiento, en particular el concepto de fuente accesible al público, así como también del hecho que no es necesario generar un registro de la finalidad para lo cual se obtiene un dato personal de dicha fuente.

"Cuando un dato se captura una fuente accesible al público no se requiere autorización del titular para efectos de tratamiento y ni siquiera se tiene que generar registro de la finalidad, la razón por la cual capturaron un dato".

En este sentido, se criticó la definición de fuente accesible al público señalando que debido a su amplitud transforma la regla general del consentimiento en una excepción. Al respecto la propuesta de la ONG Derechos Digitales es que se incorpore en la Ley un listado cerrado de aquellas fuentes que se consideran accesibles al público de manera de acotar la definición. Lo anterior, por cuanto en la actualidad incluye aquellas bases de datos que se obtienen a través de un pago a empresas.

"Es lo que sucede en España. Tú dices, las fuentes accesibles al público son, las del Conservador de Bienes Raíces, la de la guía de teléfono, etcétera. Y cualquier cosa que no esté en ese listado acotado, no es una fuente accesible al público, por tanto, requiere autorización del titular".

Por su parte, el Consejo para la Transparencia también califica como insuficiente el concepto de fuentes accesibles al público. Asimismo, dan cuenta de la complejidad de considerar cualquier registro público como fuente accesible al público, de acuerdo a la definición entregada por la Ley en el artículo 2°.

La Cámara Chilena Norteamericana de Comercio se pronunció criticando la redacción del artículo 4°, inciso 5°, que señala:

"No requiere autorización el tratamiento de datos personales que provengan o que se recolecten de fuentes accesibles al público, cuando sean de carácter económico, financiero, bancario o comercial, 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 sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios".

Lo anterior, por cuanto no existiría claridad respecto a la forma en que operan las fuentes de acceso público como excepción al consentimiento, subsistiendo la duda respecto a si dichas fuentes operan como excepción en sí mismas, además del resto de las señaladas en el inciso en comento, o deben referirse a datos con una cierta calidad. Es decir, datos que provengan de fuentes accesibles al público y que además:

- Sean de carácter económico, financiero, bancario o comercial.
- 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.
- Sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios.

Al respecto, desde la Organización Derechos Digitales dieron cuenta de que estas calidades habrían estado hechas a medida de actores del mercado como el Boletín Comercial (en el primer caso), la Asociación de Marketing Directo Chileno (en el tercer punto) y la industria en general.

"Uno de los problemas que enfrentamos en el ámbito financiero, es que básicamente lo que se busca por parte de la banca y del retail, es decir del mercado financiero en general, es tener un sistema distinto, paralelo al de los datos personales que a ellos les permita intercambiar información de forma fácil respecto de las personas".

En dicho sentido, calificaron como compleja la existencia de estas excepciones que excluye a dichos actores de las reglas generales, en especial considerando la protección que debiera existir de forma igualitaria para todas las personas respecto de sus datos personales.

"Esto puede ser problemático porque establecer excepciones para todo un sector de la industria significa establecer reglas distintas y derechos distintos que puedan ser más débiles, que puedan ser más complejos. Que tienen una justificación como en el orden público y económico, en la estabilidad del sistema, pero que en términos no se justifica como una disminución del derecho de las personas."

En particular respecto a la excepción relativa a los datos de carácter económico, financiero, bancario o comercial, dieron cuenta de la justificación de la norma pero también de los riesgos potenciales que conlleva.

"Lo importante es que el Boletín Comercial tiene una función respecto del funcionamiento de la cadena de pago. Tiene una justificación, lo importante es que esa excepción que se hace a sectores

financieros, tiene que ir sujeta al principio de finalidad (…) Esa excepción no puede extenderse a todos y cada uno de los giros de los funcionamientos del sector financiero".

En definitiva, señalan la importancia que se respete tanto el principio de finalidad en la obtención, mantención, tratamiento de datos de este tipo cuando son recolectados sin consentimiento de las personas y que se restrinja al giro comercial correspondiente en cada uno de los actores.

b) Tratamiento de datos personales por personas jurídicas privadas

El artículo 4° inciso 6° contiene otra excepción al principio general del consentimiento que se refiere al tratamiento de datos que pueden realizar 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*".

Al respecto, el Centro de Estudios de Derecho Informático de la Universidad de Chile dio cuenta, en primer lugar, de la compleja redacción que tiene la norma lo que da lugar a diferencias interpretativas, y en segundo, de su utilización abusiva por parte de un sector de la industria.

"Los hechos hoy en día, es que las asociaciones de Bancos, ISAPRES, de AFP, de Cajas, la de Universidades y las asociaciones que ustedes estimen conveniente crear pueden efectuar tratamientos entre ellas cuando es para fines de tarificación y de los propios beneficiarios. Se entiende que beneficiarios son los mismos que forman parte de esa asociación gremial, razón por la cual son un subterfugio para realizar transferencias sin autorización del titular". (CEDI)

El académico Alberto Cerda señala que esta excepción fue adoptada por el Legislador a instancias de la Asociación de Aseguradores de Chile A.G, fundado en que la circulación de información que media entre los asociados permite prevenir fraudes en seguros y adecuar la formulación de política de cobro de primas, con lo cual la excepción giraría en provecho de los propios afectados y de la comunidad toda (Cerda, 2012: p. 23).

c) Tratamiento de datos personales por organismos públicos

El artículo 20 contiene una importante excepción al principio general del consentimiento, referido al tratamiento de datos personales por parte de organismos públicos. La norma dispone lo siguiente:

"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".

El académico Alberto Cerda da cuenta de la polémica que se ha generado en torno a la extensión de las facultades que se confieren en esta norma. En este sentido, indica que una recta

interpretación obliga a considerar que la omisión de requerir la autorización del titular de los datos opera bajo dos condiciones: a) que los datos sean tratados en materia de competencia del organismo público en cuestión, lo cual excluye, por ejemplo, que un organismo de salud pública recabe datos de naturaleza tributaria; y b) que en el tratamiento en cuestión se respeten las reglas previstas por la ley (Cerda, 2012: p. 33).

Con respecto a esta excepción, el Centro de Estudios de Derecho Informático de la Universidad de Chile dio cuenta del abuso que tendría lugar en la actualidad por parte de los organismos públicos a través de la aplicación de esta norma.

"Esa decisión es monstruosa porque efectivamente se hace uso y abuso (…), en donde en general se ha desconocido una parte importante de esa norma donde dice, con sujeción a las normas presentes. Y con sujeción a las normas presentes es el principio de finalidad".

Con relación a esta materia, cabe señalar que la Ley N°19.628 contempla un registro de bancos de datos personales de organismos públicos en el artículo 22°, a cargo del Servicio de Registro Civil e Identificación.

Dicho artículo consagra el carácter público del registro y dispone que debe constar respecto de cada uno de esos bancos de datos:

- El fundamento jurídico de su existencia
- Su finalidad
- Los tipos de datos almacenados
- La descripción del universo de personas que comprende

Asimismo, se dispone la obligación del organismo público responsable del banco de datos de proporcionar estos antecedentes al Servicio de Registro Civil cuando se inicien las actividades del banco y de comunicar cualquier cambio de los elementos indicados en los puntos anteriores dentro de los quince días desde que se produzca.

Al respecto, el académico Alberto Cerda califica como lamentable la falta de sanción para aquel organismo público que no cumpla con las obligaciones establecidas en el artículo 22° de la Ley N°19.628.

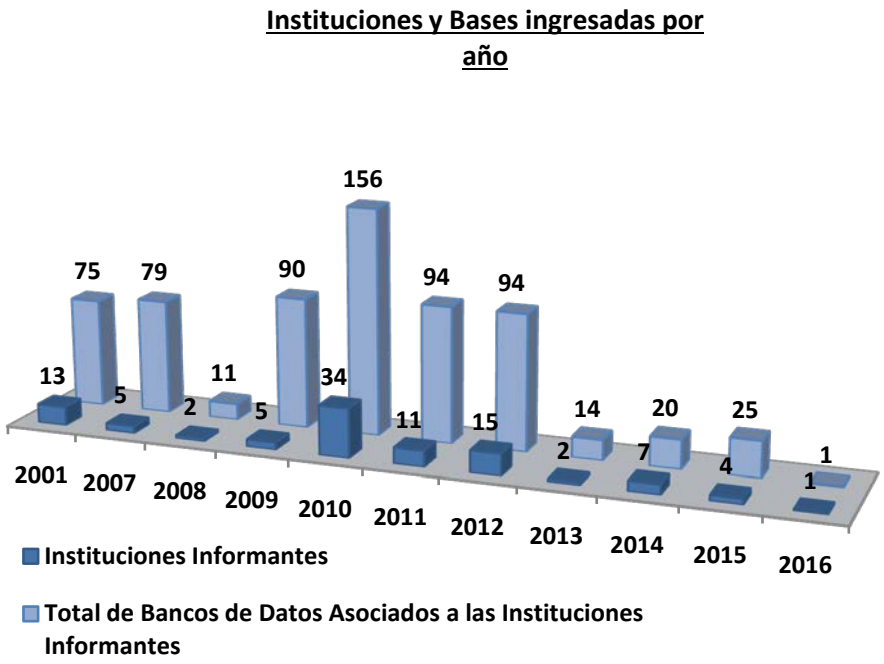
"Es de lamentar que la ley no haya establecido sanción alguna para el organismo público que omita el registro de sus bases de datos ante el Servicio de Registro Civil e Identificación, ni ha conferido a ésta repartición pública facultades para controlar el cumplimiento de tal disposición, y menos aún imponer sanciones al renuente." (Cerda, 2012: 35).

En cuanto a la aplicación de esta norma, en documento especialmente elaborado para la investigación, el Servicio de Registro Civil informó que a mayo de 2016, solo 99 organismos

públicos han informado respecto de los bancos de datos personales a su cargo, inscribiendo 659 bancos de datos en total. Por ejemplo, de las 344 Municipalidades del país, sólo 5 han dado cumplimiento a la norma.

"Como podrá advertirse los organismos públicos obligados a registrar sus bancos de datos de acuerdo con la determinación establecida en el artículo 2° letra k) de la Ley N°19.628, ascienden a aproximadamente 700, los que a lo menos debieran gestionar banco de datos personales relativos a la administración de su personal. Por ello, necesariamente debe inferirse que un porcentaje muy bajo de los organismos públicos ha cumplido con la obligación legal".

Lo anterior, se puede observar también en el siguiente gráfico, que da cuenta del bajo cumplimiento a la norma, consignando el número de instituciones informantes por año y la cantidad total de bases de datos.



Fuente: Elaboración propia con datos obtenidos del documento aportado por el Registro Civil e Identificación.

Desde el Registro Civil también señalaron que carecen de todo poder fiscalizador y sancionador para obligar a los organismos públicos a cumplir con el artículo 22° de la Ley. Asimismo, dieron cuenta del bajo porcentaje de bancos inscritos.

"Atendido el bajo número de inscripciones en el Registro de Banco de Datos a Cargo de Organismos Públicos, cabe concluir que la norma contenida en el artículo 22°, no ha cumplido con el objetivo de la integralidad, esto es que todos o un porcentaje importante de los bancos de datos personales a cargo de Organismos Públicos se encuentren inscritos".

En este orden de ideas, el Servicio señala que el cumplimiento de la normativa podría perfeccionarse, a través de la intervención legislativa, incorporando los siguientes mecanismos:

i. El otorgamiento de un plazo perentorio para la inscripción de los bancos de datos personales a aquellos organismos públicos que no lo han hecho.
ii. El otorgamiento de potestades a un organismo público para requerir información acerca del cumplimiento de esta ley a las instituciones integrantes de la Administración obligadas al registro.
iii. El otorgamiento a un organismo público de potestades de comunicación a los organismos de control ante el incumplimiento de esta obligación.
iv. El otorgamiento a un organismo público de potestades sancionatorias ante el incumplimiento de esta obligación.

Por su parte, el Consejo para la Transparencia dio cuenta de la necesidad de establecer un justo equilibrio que permita a los organismos públicos, por un lado, interoperar bases de datos personales y, por otro, respetar el principio de finalidad. Al respecto, señalaron, debiera regularse expresamente la forma, los medios y condiciones bajo las cuales los organismos públicos podrán transferir y compartir sus datos con otros organismos públicos o privados, las obligaciones asociadas, las medidas de seguridad, entre otras materias.

d) Datos sensibles con relación a beneficios de salud

El artículo 10 de la Ley N°19.628 contiene una norma que prohíbe de forma general el tratamiento de los datos personales sensibles. Sin embargo, contempla también 3 causales por las cuales es posible el tratamiento de dichos datos:

- Cuando la ley lo autorice
- Cuando exista consentimiento del titular
- En caso que sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares.

De este modo, los datos sensibles necesarios para la determinación u otorgamiento de beneficios de salud se constituyen también como una excepción al principio general del consentimiento en la Ley N°19.628. Respecto a esta causal, existe una fuerte crítica por parte de especialistas, en el sentido de que la Ley no brindaría protección suficiente a los datos sensibles.

"Se supone que el dato sensible tiene que tener un estatuto de protección mucho más riguroso que una autorización normal. Lo extraño es que en este caso además existe una excepción especial, que es para efectos de que sea necesario para el otorgamiento de un beneficio de salud". (Centro de Estudios de Derecho Informático)

En ese sentido, desde el Centro de Estudios dan cuenta de que se estaría abusando de dicha excepción y utilizando para el tratamiento de datos sensibles por parte de los actores de salud, y no ha habido una consideración de que dicha excepción fue creada para efectos del copago de salud.

"La historia de la Ley dice que esta excepción se creó precisamente para efectos del copago de salud, tiene que ver directamente con que el beneficio de salud es el beneficio para obtener de tu seguro de salud el beneficio de copago, no tiene que ver con un descuento en una farmacia".

Para la Presidenta del Instituto Chileno de Derecho y Tecnología Lorena Donoso, el estatuto jurídico de datos sensibles en la Ley N°19.628 está restringido básica y concretamente a la información de salud. De este modo, indica que no está claramente determinado en la Ley qué se entiende por *beneficios de salud*.

Al respecto, el académico Alberto Cerda también califica el régimen jurídico de los datos sensibles como exiguo, "*al punto que desdibuja la pretensión de brindarle mayor celo a su protección comparativamente respecto de los restantes datos personales*". De este modo, da cuenta de la inexistencia de niveles de seguridad asociados a la mayor o menor sensibilidad de los datos y al hecho que las formalidades y eficacia del consentimiento son similares a aquél que opera tratándose de datos personales en general. Finalmente, también sostiene que la frase *"Determinación u otorgamiento de beneficios"* resulta particularmente ambigua para fundar la excepción a la norma (Cerda, 2012:25).

6. PROCEDIMIENTO DE AMPARO DE LOS DERECHOS DE LA LEY N°19.628

La Ley N°19.628 consagra en su artículo 12 una serie de derechos que las personas pueden hacer valer frente a quienes sean responsables de un banco 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.
- **Modificación:** de aquellos datos personales erróneos, inexactos, equívocos o incompletos.
- **Eliminación:** en caso de que su almacenamiento carezca de fundamento legal o cuando estuvieren caducos, sin perjuicio de las excepciones legales.
- **Eliminación o bloqueo:** cuando la persona haya proporcionado voluntariamente sus datos o ellos se usen para comunicaciones comerciales y no desee continuar figurando en el registro respectivo, sea de modo definitivo o temporal.

El artículo 15° contempla dos importantes excepciones al ejercicio de estos derechos, disponiendo que (i) No podrán solicitarse estos derechos "*cuando ello impida o entorpezca el debido cumplimiento de las funciones fiscalizadoras del organismo público requerido, o afecte la reserva o secreto establecidos en disposiciones legales o reglamentarias, la seguridad de la Nación o el interés nacional*" y (ii) No podrá pedirse la "*modificación, cancelación o bloqueo de datos personales almacenados por mandato legal, fuera de los casos contemplados en la ley respectiva".*

Por su parte, el artículo 16° regula el procedimiento de amparo de los derechos mencionados, con dos características particulares:

- Este procedimiento sólo tiene lugar en caso que el responsable del registro o banco de datos no se pronunciare sobre la solicitud del requirente dentro de dos días hábiles, o la denegare por una causa distinta de la seguridad de la Nación o el interés nacional.
- En este caso, el titular de los datos tiene derecho a recurrir al juez de letras en lo civil del domicilio del responsable.

La sentencia que dicte el juez civil es apelable en un plazo de cinco días. El fallo que se pronuncie sobre la apelación no es susceptible de recurso de casación, existiendo un recurso de reclamación ante la Corte Suprema cuando la causal invocada para denegar la solicitud del requirente fuere la seguridad de la Nación o el interés nacional.

Con respecto a este procedimiento, los expertos e implementadores entrevistados criticaron principalmente la opción legislativa de necesaria judicialización para la resolución de conflictos que tengan que ver con protección de datos personales. En este sentido se pronunciaron desde la ONG Derechos Digitales al señalar como barrera de entrada esta circunstancia, por cuanto las

molestias o vulneraciones son apreciadas, en la práctica, como de pequeña entidad por las personas.

"Las molestias o malos ratos o vulneraciones que sufren las personas suelen ser pequeñas. Lo que ellas experimentan prácticamente. La vulneración que se realiza, en realidad es gigantesca, lo que pasa es que las personas no conocen de ella. (…) En general no es lo suficientemente alta, para que cuando la persona haga el cálculo, justifique judicializarlo". (Organización Derechos Digitales)

En un sentido similar se pronunció el abogado Nicolás Yuraszeck, señalando la complejidad de que el procedimiento de amparo de los derechos de la Ley N°19.628 tenga lugar a través de un procedimiento en sede civil, lo que incluye costear honorarios de abogados, y disponer de un tiempo excesivamente largo.

Al respecto, Derechos Digitales da cuenta de que la aplicación de la Ley se ha dado en casos muy específicos, o en casos donde organizaciones de la sociedad civil han intervenido, ya que para las personas naturales no es una alternativa viable judicializar esta materia.

Así mismo, el abogado Raúl Arrieta, destacó las complejidades al momento de acreditar los perjuicios, cuando en ocasiones el tratamiento inadecuado de información no tiene que ver con aspectos patrimoniales.

"La ley vigente, es obvio que tiene problemas del punto vista que no tiene mecanismos para hacer efectivos los cumplimientos. Hoy día el costo transaccional de reclamar la infracción del derecho es tan alto que la gente no reclama".

Además, el abogado manifestó la necesidad de que exista una entidad administrativa que aplique sanciones de ese mismo carácter, y que luego las personas tengan el derecho de acudir a tribunales para efectos de reclamar los perjuicios ocasionados.

Asimismo, el académico constitucionalista Flavio Quezada también se manifestó señalando la poca efectividad del mecanismo judicial, considerando los costos de litigación. Asimismo, hizo mención a las facultades del Consejo para la Transparencia en materia de protección de datos.

"Si bien en Chile nuestro Consejo para la Transparencia tiene algunas atribuciones en esta materia, súper genéricas respecto de los organismos públicos, uno no puede decir que genuinamente se haya constituido como agencia de protección de datos personales".

En documento aportado a la investigación, el Consejo para la Transparencia dio cuenta que las desventajas del procedimiento de amparo han provocado que los operadores jurídicos recurran por medio del recurso de protección a los tribunales de justicia, invocando la vulneración de la privacidad como derecho fundamental. Asimismo, señalaron la existencia de problemas respecto 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; finalmente no se establece un plazo de prescripción de la acción con lo que se afecta la seguridad jurídica".

En el mismo sentido se pronunciaron desde el Centro de Estudios de Derecho Informático de la Universidad de Chile, al señalar la importancia de contar con una entidad administrativa intermediaria, que ejerza los derechos que la ley consagra, equilibrando la situación entre el titular de los datos y el responsable del registro e imponiendo las sanciones que correspondan.

"El tener una autoridad de control no es un capricho, no es antojadizo, es que efectivamente como país nos merecemos tener un ente administrativo que equilibre lo que existe de asimetría entre las partes".

Asimismo, desde el Servicio Nacional del Consumidor (SERNAC) también dieron cuenta de la necesidad de una autoridad reguladora supervisora del cumplimiento de las disposiciones de la Ley. En particular, señalaron que la regulación actual del procedimiento de amparo a través de la justicia civil, no sería un mecanismo eficiente, considerando el carácter técnico de esta materia.

En definitiva, si bien existe en la Ley un procedimiento de amparo de los derechos, por su diseño y regulación, y al implicar una carga para el afectado de tal envergadura, esto no cumple su objetivo.

7. SANCIONES EN LA LEY N°19.628

Los dos últimos incisos del artículo 16 facultan al juez civil para aplicar las siguientes sanciones:

- Multa de 10 a 50 UTM en caso de las infracciones a los artículos 17° (infracción a la prohibición de comunicación de ciertas deudas) y 18° (infracción a la prohibición de comunicación de datos comerciales luego de transcurridos cinco años desde que la obligación se hizo exigible, o respecto de obligaciones ya extinguidas).
- Multa de 2 a 50 UTM, para la falta de entrega oportuna de la información o el retardo en efectuar la modificación en la forma que decrete el tribunal.
- Multa de 1 a 10 UTM, en el resto de los casos.

Con relación al aspecto sancionatorio, la Organización Derechos Digitales criticó la falta de catálogo de infracciones en la Ley y el hecho que las sanciones actuales con bajas. Asimismo, señalaron que frente a fallas de seguridad que han tenido lugar en ciertos Bancos, que han resultado en fugas de datos, no ha existido sanción y de existir, tendrían lugar multas de muy poca cuantía.

"No existen mecanismos para una reclamación efectiva por la infracción a deberes de la Ley de datos personales. Y además, no existen sanciones asociadas a ellas".

Frente a esto, dan cuenta de la necesidad de incorporar un catálogo de infracciones que operen como incentivo para las empresas para velar de forma óptima por la seguridad en el tratamiento de los datos personales que manejan.

"Se echa de menos un catálogo de infracciones en la ley, que un poco, sirvan de detrimento para las empresas a cumplir con estos deberes. Acompañado de su carácter indemnizatorio".

En sentido similar se pronunciaron desde la Cámara de Comercio de Santiago, quienes, en documento especialmente elaborado para la investigación, declararon:

"Faltan instrumentos de control de los titulares sobre sus datos personales y hay bajas posibilidades de aplicar sanciones frente a las infracciones que la ley establece".

Con relación a lo anterior, el abogado experto Raúl Arrieta dio cuenta de la falta de incentivos para las empresas u organismos públicos que se enfrentan a un *data breach* de informar a los titulares de los datos personales de la ocurrencia de un hecho que permitió la fuga de datos. En particular, menciona la filtración ocurrida al Ministerio de Salud.

"Hasta el día de hoy no veo un anuncio del Ministerio de Salud informando a los titulares que sus datos pueden haber sido expuestos para que esa persona vuelva a tomar el control de sus datos y pueda tomar acciones concretas para proteger su información".

Respecto a estas fugas de datos, el especialista da cuenta de un vacío en la legislación actual ya que no existen normas que regulen de forma apropiada la obligación para quien trata datos de adoptar medidas de seguridad acorde con el tipo de datos que trata.

"No es lo mismo un almacenero tratando datos, que Equifax tratando datos o un banco tratando datos. En un caso tenemos expertos en tratamiento de datos y en el otro lado tenemos un almacenero. Entonces obviamente eso requiere estándares diferentes".

Asimismo, dio cuenta de la necesidad de incorporar normas que obliguen a dar aviso a los titulares de los datos cuando ha tenido lugar una fuga, junto con sanciones que incentiven a las empresas u organismos públicos a dar este aviso, de modo que las personas titulares de los datos puedan tomar los resguardos necesarios y se disminuya el perjuicio.

"Lo que las legislaciones hacen es sancionar el que tú no hayas avisado que expusiste datos, no el que los expongas porque eso siempre puede pasar".

En sentido similar se pronunció el abogado experto Carlos Reusser, quien señaló que frente a las brechas de seguridad no existen actualmente incentivos para informarlos. Para esto, indicó que es necesario incorporar un sistema de notificaciones como también incentivos para que quienes tratan datos comuniquen este hecho a los titulares.

"Para que en definitiva las sanciones, por no decir nada, sean mucho más duras que las que dan el pronto aviso para que la gente tome las providencias que mejor puedan".

Asimismo, el abogado especialista Nicolás Yuraszeck dio cuenta de la falta de incentivos que existen hoy en día para el sector público y privado de cumplir con la ley, en especial considerando la baja cuantía de las multas y la radicación del procedimiento en sede civil, lo que puede implicar varios años de tramitación y elevados costos para el afectado.

De forma similar se pronunciaron desde el Centro de Estudios de la Universidad de Chile, indicando la falta de operatividad de la Ley y la falta de cumplimiento de sus objetivos.

"Tiene un estatuto de control y un estatuto sancionatorio que es ineficaz y precario y la transforma en muchos aspectos prácticamente en letra muerta".

En síntesis, si bien existen multas consagradas en la Ley para quienes no respeten los derechos que el procedimiento ampara, la baja cuantía de estas hace que no operen correctamente como incentivos al cumplimiento de la Ley.

8. DERECHO AL OLVIDO

El derecho al olvido es un tema en constante debate doctrinario en todos los lugares en donde se plantee. Es un derecho en formación, no están claros ni sus límites ni su extensión. Ya su nombre a muchos les genera incomodidad.

La Real Academia Española lo define como "*Cesación de la memoria que se tenía"*, por tanto desde una primera vista podemos decir que este derecho debería considerar suprimir un recuerdo, la memoria o información.

Luis Mieres (2014) sostiene que el reconocimiento del derecho al olvido busca garantizar la efectividad del control de las personas sobre las informaciones y datos presentes en la red que se refieren a ellas, que resultan obsoletas y cuya difusión o accesibilidad actual les perjudica.

Cécile de Terwangne (2012) señala que es el derecho de las personas físicas a hacer que se borre la información sobre ellas después de un período de tiempo determinado.

En una dirección similar se pronuncia la Sección Asesoría Técnica Parlamentaria de la Biblioteca del Congreso Nacional, indicando que puede entenderse por derecho al olvido la facultad irrenunciable del titular de datos de solicitar el bloqueo, supresión o eliminación de toda información relativa a su persona, cuya publicación es extemporánea, no veraz o la perjudica.

La Agencia Española de Protección de Datos entiende que el denominado derecho al olvido es la manifestación de los tradicionales derechos de cancelación y oposición aplicados a los buscadores de internet, es decir, el derecho a impedir la difusión de información personal a través de internet cuando su publicación no cumple los requisitos de adecuación y pertinencia previstos en la normativa e incluye el derecho a limitar la difusión universal e indiscriminada de datos personales en los buscadores generales cuando la información es obsoleta o ya no tiene relevancia ni interés público, aunque la publicación original sea legítima.

Por último la Excma. Corte Suprema de nuestro país, en un fallo reciente[5] en que por primera vez reconoce el derecho al olvido, ha indicado al respecto que se refiere sustancialmente a que una persona pueda aspirar a la eliminación de una información desfavorable sobre sí misma que le provoque perjuicios actuales y que se contenga en los sistemas informáticos disponibles, y ello por una razón plausible.

a) Caso *Costeja con Google*

En España, en el año 1998 el periódico *La Vanguardia* publicó un anuncio de subasta de varios inmuebles embargados por la Secretaría de Seguridad Social. Dicho anuncio incluía la ubicación del inmueble, sus características y el propietario. Posteriormente, alrededor de una década después, el periódico comienza el proceso de digitalizar todas sus ediciones, generando así la posibilidad de que los motores de búsqueda indexen los datos contenidos en aquellas ediciones digitalizadas. Uno de esos propietarios, cuyo inmueble estaba publicado para ser subastado, era el señor Mario Costeja González, el cual en una búsqueda de su nombre mediante el motor *Google*, se encontró con que aquella página de periódico donde se realizó aquel anuncio aún estaba disponible para ser visto por cualquiera, de forma digitalizada.

Este señor ejerció su derecho de oposición ante el periódico, lo que le fue denegado por éste debido a que en su oportunidad a la publicación se había realizado en forma lícita, tal como la legislación lo contemplaba para una subasta. Ante esta situación, solicitó al motor de búsqueda señalado que suprimiera la información, obteniendo la misma respuesta negativa.

Costeja persistió y accionó las vías disponibles, es decir la administrativa ante la Agencia Española de Protección de Datos Personales, la que rechazó la oposición contra el periódico, sin embargo la admitió contra el buscador, es decir, la empresa *Google*. Ante esto, dicha empresa recurrió a la Justicia Española solicitando la nulidad de dicha resolución. Así, en el año 2012 el tribunal que

[5] Sentencia Rol Nº 22.243-2015, del 21 de enero del 2016 de la Excma. Corte Suprema.

debía dirimir el conflicto optó por enviar una consulta al Tribunal de Justicia de la Unión Europea, generándose así el fallo que reconoció por primera vez el denominado derecho al olvido.

Esto ocurrió el día 13 de mayo del año 2014 en que el Tribunal de Justicia de la Unión Europea se pronunció ante la controversia y estableció que mediante la interpretación de la Directiva 95/46/CE era posible configurar el derecho al olvido (desde los derechos de oposición y cancelación), obligando a G*oogle* a no mostrar la publicación al buscar con el nombre del reclamante, sin disponer la eliminación de la noticia.

b) ¿Intimidad o protección de datos personales?

Podemos encontrar que en la configuración del *Olvido* hay posturas opuestas en relación con los derechos a los que este se vincularía. Algunos sostienen que el derecho al olvido se funda en el derecho a la vida privada y a la honra, mientras que otros postulan que se proyecta desde el derecho a la protección de datos.

Lo anterior marca diferencias, pues según la primera postura, una información obsoleta del pasado podría vulnerar bienes jurídicos protegidos por la intimidad o el honor, forzando así una amplia interpretación en su ámbito de protección. Mientras que la segunda tiene por objeto de protección directamente de los datos personales, lo que enmarca un espectro de protección más amplio, atendiendo a la propia definición de dato personal.

También tiene relevancia por cuanto la privacidad y la honra tienen rango constitucional expreso, con las garantías que eso genera, como la posibilidad de interponer un recurso de protección ante la Iltma. Corte de Apelaciones respectiva. Mientras que la protección de los datos personales se encuentra presente en la Ley N°19.628 sobre protección de la vida privada, el que contempla un procedimiento de reclamación (para ejercer los derechos establecidos en la misma normativa) ante los tribunales civiles ordinarios.

La Excma. Corte Suprema, en un reciente fallo de fecha 21 de enero de 2016[6], se inclina por la percepción del derecho al olvido fundado en el derecho a la privacidad y a la honra. Tal vez esto se debe a que se trata de un recurso de protección y, por consiguiente, la discusión se centra en los derechos fundamentales garantizados mediante este recurso, los que en este caso son principalmente la privacidad y la honra. Así se manifiesta en el considerando cuarto:

"No cabe duda que nuestro ordenamiento jurídico protege el honor y vida privada de las personas en cuanto tales, incluso antes y después de su constitución jurídica; y que sistemáticamente ha venido recogiendo la tendencia mundial de reconocer el derecho al olvido respecto de conductas

[6] Sentencia Rol Nº 22.243-2015, del 21 de enero de 2016 de la Excma. Corte Suprema

reprochables de las personas –sean éstas penales, civiles o comerciales- después de un lapso de un tiempo, como una forma de reintegrarlas al quehacer social". (Excelentísima Corte Suprema)

Sin embargo, como sostiene el destacado académico Rodrigo Moya, especialista en derecho informático y miembro del Centro de Estudios en Derecho Informático de la Universidad de Chile, es innegable que existe una relación de género-especie entre privacidad y datos personales.

"No podemos decir que no se vinculan, pero están en una relación de género-especie. Datos personales se descuelga de una garantía fundamental que es privacidad, pero intimidad, privacidad, derecho a la propia imagen, derecho a la vida privada es superior, es mucho más allá que solo tratamiento de datos personales". (Centro de Estudios en Derecho Informático de la Universidad de Chile)

La tendencia moderna, reflejado en el Reglamento de Protección de Datos de la Unión Europea, es vincular el derecho al olvido o supresión, a la protección de datos personales, pues dice relación directa con el objeto del derecho.

c) Conflicto

Se suele confrontar este derecho al olvido con la libertad de expresión o libertad informativa, configurándose en una especie de censura legal. Es evidente que tanto la protección de datos como la libertad de expresión tienen un elemento central en común, la información. Pero no siempre toda información tiene datos personales, por tanto el conflicto no es total, sino solo en cuanto a aquella que contenga datos personales.

En razón de lo anterior, el profesor Pablo Salvador Coderch expresó en una columna del periódico español El País que *"La censura retroactiva de los medios de información es la cara oscura del pretendido derecho al olvido. Su consagración legal produciría efectos perversos e imprevistos por muchos de sus proponentes"*[7].

La Excma. Corte Suprema también reconoce que el derecho al olvido (en ese caso vinculado a la privacidad y la honra) puede colisionar con el derecho a la libertad de expresión, aunque recoge un criterio para realizar el ejercicio de ponderación, este es el transcurso del tiempo. En el fallo rol Nº 22.243-2015, indica que:

"No debe escudriñarse una real colisión entre dos garantías constitucionales aparentemente contrapuestas, a saber: El derecho al olvido, como protección del derecho a la integridad síquica y a la honra personal y familiar, frente al derecho de informar y de expresión. Cada uno tiene una

[7] Diario El País. Tribuna: Entre Recordar y Olvidar. Publicado el día 1 de junio de 2011.

esfera de acción propia que puede llegar a superponerse durante un tiempo, en el que es necesaria y útil la información pública frente al derecho personal que pueda invocarse, pero que decae con la extensión de dicho transcurso de tiempo; y en cambio deviene en atrabiliaria e inútil tanto para el derecho del individuo afectado para reintegrarse a plenitud a la sociedad, como para esta última de conseguir la pacificación que le interesa primordialmente y que una noticia caduca no facilita". (Excma. Corte Suprema)

Finalmente, la Corte reflexiona que después del tiempo transcurrido, ante la colisión entre los dos derechos fundamentales aludidos debería ceder la libertad de expresión, a favor de la reinserción social y del derecho a mantener una vida privada que posibilite el ejercicio del primero, como asimismo el derecho a la honra y privacidad de su familia.

En atención a la posibilidad de generar un abuso del derecho al olvido sobre la libertad de expresión, es que el Reglamento General de Protección de Datos de la Unión Europea (Reglamento 2016/679) considera que no procederá el derecho a la supresión (o derecho al olvido) en las ocasiones en que la conservación de los datos sea necesaria para el ejercicio del derecho a la libertad de expresión. Esto busca poder conciliar la existencia de un derecho al olvido y la libertad expresión necesaria en toda sociedad informada.

d) La situación en Chile

Como se ha mencionado anteriormente, el fallo Rol Nº 22.243-2015 de la Excelentísima Corte Suprema se considera como el primero en reconocer y aplicar el denominado derecho al olvido. Aunque no lo hace desde la Ley N°19.628 y los derechos de oposición y cancelación ahí contenidos, sino desde la perspectiva de la privacidad en su esfera de protección constitucional.

En este caso, una persona solicita ser eliminado del archivo digital de un medio de comunicación, debido a que éste último tiene un registro noticioso en que se informa de la condena del sujeto por determinados delitos.

Así en su considerando cuarto señala: *"Que en nuestro ordenamiento jurídico nacional no existe, por ahora, una solución legislativa expresa sobre este tema, aunque no resulta difícil advertir en él su compromiso con la protección del honor, la dignidad y vida privada de las personas".* (Excma. Corte Suprema)

Además de la posición del tribunal, es necesario mencionar que en la actual Ley de protección de la vida privada, están contenidos los denominados derechos ARCO, es decir, los derechos de acceso, rectificación, cancelación y oposición, siendo los últimos dos los que más se vinculan en la conformación del derecho al olvido. Por tanto, se podría sostener que existen las bases para que doctrinaria o jurisprudencialmente se pueda configurar desde ahí un derecho al olvido vinculado a la protección de datos personales.

Así lo expresó Andrea Ruiz, directora jurídica del Consejo para la Transparencia al indicar que *"El concepto de derecho al olvido se construye doctrinariamente, pero el derecho al olvido se traduce en derechos de las personas, como la cancelación o bloqueo de mis datos por estimar que son caducos".* (Consejo para la Transparencia)

Algunos también sostienen que ya en el año 2012 se adoptó de forma tácita el derecho al olvido, en el fallo[8] referido a un recurso de protección dictado por la Ilustrísima Corte de Apelaciones de Valparaíso. Se trata de una persona que presentó dicho recurso en contra de los administradores de una serie de sitios web, puesto que en ellos se difundía información falsa que la comprometía y a su familia, fundado en los derechos de la privacidad y honra, solicitando por consiguiente la eliminación de toda dicha información injuriosa.

En este caso la Corte lo acogió, señalando "*Que el buscador google.cl establezca computacionalmente, los filtros necesarios, para evitar publicaciones que presenten inequívocamente publicaciones de carácter injurioso, o de cualquier tipo y bajo cualquier circunstancia, siempre que en esa publicación se incurra en una afectación como la de autos*". (Ilustrísima Corte de Apelaciones de Valparaíso)

Como se observa ya han existido ocasiones en donde se configura tácitamente el derecho al olvido, o bien, de forma expresa como en el primer caso. Sin embargo, se han vinculado ambos casos a la vida privada y la honra, a pesar de la posibilidad de configurarlo desde la protección de datos personales y sus respectivos derechos de cancelación y oposición.

[8] Causa 228/2012, Ilustrísima Corte de Apelaciones de Valparaíso.

CAPÍTULO IV. CONTROL Y FISCALIZACIÓN DE LA NORMA

La ausencia de una institución que eduque, controle y fiscalice la protección de datos personales con un alcance transversal a todos los actores que tratan información de estas características, es indicada como una de las principales debilidades de la norma en Evaluación.

Durante sus 17 años de vigencia, se han realizado diversos intentos para efectuar modificaciones profundas a la legislación chilena en materia de protección de datos. Sin embargo, dichos esfuerzos no han logrado concretarse en un proyecto de Ley que culmine su tramitación legislativa en el Congreso Nacional.

En el presente capítulo, se revisan algunos de los hitos que han marcado la discusión sobre la modificación de la Ley, considerando su relevancia en el debate público, así como la participación de actores provenientes de diversos sectores en las distintas instancias.

Además, se analiza desde la perspectiva de los entrevistados para esta evaluación el papel desempeñado por el Consejo para la Transparencia como la única institución llamada a velar por el complimiento de la norma por parte de las instituciones públicas.

La ausencia de fiscalización y la escasa educación en materia de protección de datos personales son otros de los temas de los que se da cuenta en este capítulo, siendo relevantes para comprender la percepción de desconfianza que posee la ciudadanía.

Se recoge, también, la experiencia de autorregulación comentada por las instituciones privadas como una vía mediante la cual las empresas han buscado aunar criterios para la aplicación de la norma.

Finalmente, se exponen las diversas propuestas para la generación de un organismo de control que dé garantías de una protección de datos personales que cumpla con las exigencias internacionales.

1. INICIATIVAS DE MODIFICACIÓN DE LA LEY N°19.628

Diversos han sido los intentos efectuados por el Poder Ejecutivo y Legislativo para modificar esta norma. Una consulta pública y un número importante de mesas de diálogo integrada por actores provenientes del mundo académico y empresarial forman parte de un largo recorrido que, desde la perspectiva de los entrevistados, no ha entregado resultados concretos. Sin embargo, este andar ha dejado de manifiesto la necesidad de potenciar cambios que propendan a dotar de un marco legal más robusto en materia de protección de datos personales.

A continuación se describen algunos de los hitos que han marcado la discusión en torno a la protección de datos personales en nuestro país.

- **Desarrollo productivo y servicios globales**

Las primeras iniciativas que centraron su atención en el tratamiento de datos personales, surgen en el ámbito del comercio internacional, relacionados principalmente con la Industria de Servicios Globales u offshoring.

En 2008, con el apoyo del Consejo Nacional de Innovación para la Competitividad, se encomienda a la Corporación de Fomento de la Producción (CORFO) la coordinación de un plan de desarrollo productivo focalizado, también conocido como Programa Nacional de Clusters, en el que se buscaba potenciar el crecimiento y competitividad de diversos sectores, entre ellos los Servicios Globales.

En 2010 Chile se potencia como una localización atractiva para empresas multinacionales que desean operar desde fuera de sus territorios de origen, a través de plataformas tecnológicas que posicionan el tratamiento de datos como su principal herramienta. Es en este marco, que el Consejo Estratégico Público –Privado de Cluster, creado para esos efectos, establece como un punto central de la segunda fase de implementación del programa un Comité de Regulación destinado a generar una propuesta de modificación legal.

Durante dicha instancia se conformó una mesa de trabajo en la que participaron representantes del Ministerio de Economía, Fomento y Turismo, CORFO y la Secretaría General de la presidencia (SEGPRES). De esta iniciativa surgiría un convenio de colaboración técnica con la Agencia Española de Protección de Datos y se incorporarían indicaciones al proyecto de Ley de Transparencia.

Consejo Estratégico del Cluster de Servicios Globales	
Representantes de Empresas	**Representantes de Asociaciones Empresariales**
Jaime Pacheco, Gerente General de ORACLE Pablo Quezada, Gerente General TELEPERFORMANCE Mohit Srivastava, Gerente General de EVALUESERVE Víctor Grimblatt, Gerente General de SYNOPSYS	Raúl Rivera, Presidente Foro Pro Innovación Raúl Ciudad y Miguel Pérez, PastPresident y Presidente de la Asociación de Empresas de Tecnología de Información (ACTI) Mateo Budinich y Ricardo García, PastPresident y Presidente de la Cámara Chileno Norteamericana de Comercio (AMCHAM) Elías Arce, Representante de la Asociación de los Ingenieros Consultores (AIC)
Representantes de Instituciones de Educación Superior	**Representantes del Sector Público**
Hernán de Solminihac, Decano de la Facultad de Ingeniería de la Universidad Católica de Chile Gonzalo Vargas, Rector del INACAP	Carlos Álvarez, Vicepresidente Ejecutivo de CORFO Orlando Jiménez, Representante del Ministerio de Economía Sonia Zavando, Representante del Ministerio de Educación Osvaldo Marinao, Representante de PROCHILE

Fuente: Elaboración propia con datos obtenidos en presentación de CORFO titulada *Balance Consejo Estratégico del Cluster Servicios Globales*

Sobre este tema se pronuncia la Fundación Datos Protegidos, aludiendo al proyecto ingresando durante el primer mandato de la Presidenta Michelle Bachelet en el año 2008 y narrando el momento en que la protección de datos recae en el Ministerio de Economía.

"[La compañía telefónica] *le pasa la base de datos de sus clientes a una empresa en Colombia, y esa empresa en Colombia los procesa. En Europa eso se hace mucho y solamente ellos lo hacen con países que se consideran de protección adecuada, que en Latinoamérica serían dos: Argentina y Uruguay, nosotros no. Chile empezó a pensar en esto, esto nos puede traer más empleos. Mientras los europeos duermen nosotros estamos despiertos, podemos trabajar, y se empezó a generar este boletín* [Boletín 6120-07] *como para poner en una agenda de impulso a los servicios globales, por eso el proyecto cae en Economía".*

- **Se mantiene el enfoque financiero**

La elaboración de un nuevo proyecto de ley en 2010, durante un segundo intento del Ejecutivo por modificar la norma, mantendrá el enfoque financiero característico de la ley de protección de datos desde su nacimiento.

"En Chile teníamos esta norma que establecía un capítulo especial para el tratamiento de datos financieros, o sea, regulaba básicamente a DICOM y todas estas empresas que cobran. Finalmente es un procedimiento, que empezamos a ver si se ejercía o no, si, las personas cuando se sentían

como vulneradas, iban o no a tribunales. Y la mayoría de los juicios, son por DICOM, son por publicaciones erróneas en DICOM; porque yo ya no debía y todavía parecía publicado. Unos juicios se ganaban, otros juicios, la mayoría, terminaba en conciliaciones en la primera audiencia (Fundación Datos Protegidos).

Es en el gobierno del ex presidente Sebastián Piñera, que se impulsará un nuevo proyecto de ley, siendo el Ministerio de Economía nuevamente el encargado de retomar el tema. Durante este periodo surge interés por el Servicio Nacional del Consumidor (SERNAC) como organismo fiscalizador de la norma, ante la ausencia de uno establecido expresamente en la Ley N°19.628. No obstante, su denominación es criticada por los actores involucrados.

"Del proyecto del año 2012, una de las cosas que se mencionó durante la discusión es entregar atribuciones administrativas al SERNAC. Lo cierto es que el SERNAC, ya en el ámbito de los derechos del consumidor es débil, porque toma algunas acciones pero no resuelve y no sanciona. Entonces no es un modelo a seguir el SERNAC, si no un modelo administrativo más fuerte. (Organización Derechos Digitales)

- **Participación de actores de diversos sectores marca el debate**

Junto a la nueva administración de la Presidenta Michelle Bachelet surge otra propuesta para mejorar el cuerpo normativo en materia de protección de datos. La elaboración de un nuevo proyecto es liderado por la entonces Subsecretaria de Economía, Katia Trusich, quien realizará diversas actividades con el objeto de recoger las opiniones y propuestas desde la Industria, la Sociedad Civil, la Academia y de ciudadanos interesados en participar.

Entre ellas, se destaca una consulta pública realizada en 2014 a través el sitio web del Ministerio en que se contó con la participación de los siguientes actores: Telefónica Chile S.A, SICC Ltda., Microsoft, Instituto Chileno de Derecho y Tecnologías, Hewlett Packard Chile Comercial Limitada, ONG Derechos Digitales, Databusiness, Colegio de Bibliotecarios de Chile A.G., Cámara Nacional de Comercio, Claudio Ragni, Claudio Magliona, Asociación Chilena de Empresas de Tecnología de la Información, Information Technology Industry Council, Fundación Hacer Chile, Google Yahoo y Mercado Libre, entre otros.

"Se hizo efectivamente una Consulta Pública, se recibieron más de 460 comentarios, hubo participaciones interesantes, se mandaron comentarios súper buenos, súper importantes. (…) Y aparte de esa Consulta, se constituyó una mesa público-privada donde participaron un montón de instituciones donde básicamente lo que hicimos fue revisar el proyecto que se sometió a Consulta Pública" (Raúl Arrieta, asesor Ministerio de Economía año 2014)

Los contenidos del anteproyecto sometidos a Consulta Ciudadana, se detallan en el siguiente recuadro:

Títulos	Contenido
Título I	Disposiciones Generales
Título II	Principios del Tratamiento de Datos Personales
Título III	Derechos de las Personas
Título IV	Otras Disposiciones
Título V	Datos especialmente Protegidos
Título VI	Transferencia Internacional de Datos Personales
Título VII	Del Registro Nacional de Bases de Datos
Título VIII	Del Consejo para la Protección de Datos
Título IX	Infracciones y Sanciones
Disposiciones Transitorias	

Fuente: Sitio web http://www.participacionciudadana.economia.gob.cl/

Durante la misma fecha en que fue ejecutada la Consulta Ciudadana, se organizan mesas de trabajo con la participación de actores del mundo público, privado, académico y aquellos pertenecientes a organizaciones no gubernamentales con el fin de discutir algunos aspectos tratados en ella.

"Nosotros, participamos con la Subsecretaria en muchas reuniones y estuvimos también presentes cuando la Subsecretaria presentó las bases centrales para lo que iba a ser el proyecto de ley (…) primero bajo la necesidad de adecuarse a los estándares de la OCDE, y segundo, porque la que teníamos no sirve" (Organizaciones de Consumidores)

A continuación se exponen los actores que participaron de las mesas de trabajo:

Nombre	Cargo	Institución
Segismundo Schulin-Zeuthen S.	Presidente	Asociación de Bancos e Instituciones Financieras
Ricardo Mewes	Presidente	Cámara Nacional de Comercio
Peter Hill	Presidente	Cámara de Comercio de Santiago
Claudio Ortíz	Gerente General	Comité de Retail Financiero
José Manuel Camposano	Presidente	Asociación de Aseguradores de Chile
Carlos Reusser	Consejero	Instituto Chileno de Derecho y Tecnologías
Federico Allendes	Presidente	Pro Acceso

Nombre	Cargo	Institución
Jaime Soto	Presidente	ACTI
Davor Harasic	Decano	Facultad de Derecho de la Universidad de Chile
Guillermo Carey	Presidente	AMCHAM
Boris Tirado	Presidente	Digital AG
Romina Garrido	Presidente	Fundación Datos Protegidos
Hernán Calderón	Presidente	CONADECUS
Paula Jaramillo	Investigadora	Derechos Digitales
Alejandro Micco Aguayo	Subsecretario	Ministerio de Hacienda
Cristián Ocaña Alvarado	Presidente	Colegio de Ingenieros de Chile A.G.

Fuente: Elaboración propia con información aportada por la Asociación Chilena de Empresas de Tecnología de la Información A.G. (ACTI)

Según se indicó, el trabajo llevado a cabo en aquellas mesas forjó consensos importantes entre los participantes en relación a buena parte de su contenido, situación que fue destacada por los entrevistados para esta investigación. Así lo señaló el abogado Carlos Reusser, al momento de referirse al trabajo realizado.

"*Hace unos dos años atrás, a instancias del Ministerio de Economía, nos reunimos para consensuar un proyecto de ley. Llegamos a un acuerdo global entre, la industria, la Cámara de Comercio, la Universidad, las ONG. Era un consenso casi absoluto, algunos reclamaban si la multa era muy baja o era muy alta, pero fue un consenso".*

Por su parte, Arrieta, asesor del Ministerio de Economía durante este periodo, también puso énfasis en el consenso obtenido,

"Ahí hicimos un trabajo donde fuimos revisando artículo por artículo, y yo me atrevería a decir que en ese proyecto de ley hay un consenso del 90%, 95%. Porque, obviamente la banca y el retail nunca las voy a poner de acuerdo con el dato económico y es por eso que el objetivo de ese proyecto de ley era generar un debate pre-legislativo que dejara a todos estos actores tranquilos en el grueso y los intereses particulares que tuviera cada uno que lo quisieran abrir en el Congreso y que se discutiera, pero era un proyecto que tenía una unanimidad y consenso absoluto en lo que tenía que ver con ámbitos de aplicación, con principio, con derecho, con autoridad de protección de datos, con las sanciones". (Raúl Arrieta, asesor Ministerio de Economía año 2014)

A pesar de lo expuesto y de la prevalencia de aquel consenso, el proyecto de ley no fue enviado al Congreso, desconociéndose el grado de integración de este trabajo a nuevas instancias de modificación, así como la continuidad de las mesas de trabajo.

- **Nuevo compromiso del gobierno e influencia de la OCDE**

El 11 de Mayo de 2015, durante el segundo periodo de la Presidenta de la República Michelle Bachelet, se presenta la Agenda de Probidad y Transparencia en los Negocios y Política, como parte de su compromiso para reconstruir confianzas. La Agenda se compuso por 14 medidas administrativas que serían implementadas durante el transcurso de 15 días y 21 iniciativas legislativas, expresadas en proyectos de ley e indicaciones, que ingresarían al Congreso durante los siguientes 45 días.

Dentro de estas iniciativas legislativas destacaba la protección de datos personales, medida que se expresaba conforme a las garantías que debían existir en la protección de los derechos de las personas en esta materia, asegurando, entre otras cosas, la igualdad en el tratamiento de éstos.

En junio de 2015, el Ministro de Hacienda, Rodrigo Valdés da cuenta de uno de sus compromisos: acortar la agenda legislativa a aquellos proyectos que eran prioritarios para impulsar el crecimiento del país, entre ellos anuncia el Proyecto de “Protección de Datos Personales” como una de las 19 iniciativas claves consideradas para este proceso.

Es importante destacar que la Organización para la Cooperación y el Desarrollo Económico (OCDE), envió una carta de recomendación al Ministerio de Economía de Chile por el retraso que existía en el país en temas de protección de datos personales, acuerdo sellado en 2010 como parte del compromiso adquirido para ingresar al organismo internacional.

Actualmente, el Ministerio de Hacienda se encuentra elaborando otro proyecto de ley, del que hasta la fecha sólo se ha conocido una minuta publicada en los medios que en principio integraría algunos de los consensos obtenidos en instancias anteriores tales como la creación de un organismo de control, regulación del consentimiento, obligaciones del responsable de datos entre otros. Al momento de la publicación de este informe, el proyecto de Ley no ha sido ingresado al Congreso Nacional.

2. ORGANISMO DE CONTROL PARA LA PROTECCIÓN DE DATOS PERSONALES

El texto legal que regula el tratamiento de datos personales en Chile no hace referencia explícita entre sus articulados a una institución que vele por el cumplimiento de la norma. Según señala Alberto Cerda, abogado y académico experto en derecho y tecnología de la Universidad de Chile:

"Durante la tramitación parlamentaria de la Ley 19.628 la Comisión de Constitución, Legislación y Justicia del Senado estimó erradamente que la tendencia legislativa era prescindir de una autoridad de control en la materia, sobre la base de tres consideraciones: la proliferación de los computadores, lo que hacía imposible verificar control sobre el tratamiento de datos; la incapacidad de la autoridad central para detectar empleo inadecuado de los datos contenidos en las bases; y el creciente movimiento internacional de datos, que hacía infructuosos los esfuerzos limitados al ámbito territorial de competencia de una autoridad semejante". (Cerda, 2012: 37)

Existe consenso entre los entrevistados de esta evaluación que uno de los nudos críticos que presenta la Ley N°19.628 es la inexistencia de un autoridad administrativa que eduque, fiscalice y controle el cumplimiento de la norma tanto para instituciones públicas como privadas.

"Chile lo que hizo fue tomar la LORTAD, la ley española y meterla en un modelo más parecido al sistema norteamericano. (…)Estableció ciertos principios, muy acordes a la legislación internacional. Sin embargo, omitió dos o tres elementos esenciales. El primero fue la autoridad de control, o sea en el fondo nació una ley con estatus jurídico sin una autoridad de control, sin una autoridad que velara por el cumplimiento de la ley". (Lorena Donoso, Instituto Chileno de Derecho y Tecnología)

a) Consejo para la Transparencia llamado a velar por la protección de datos personales

Será en una discusión más tardía, transcurridos 9 años de su entrada en vigencia, y en el marco de la publicación de la Ley N°20.285 sobre Acceso a la Información Pública, que crea al Consejo para la Transparencia, que se encomendó en su artículo 33° a dicha institución *"Velar por el adecuado cumplimiento de la Ley Nº 19.628, de protección de datos de carácter personal, por parte de los órganos de la Administración del Estado"*

De esta manera, el organismo recientemente creado para garantizar el derecho de acceso a la información debe, además, resguardar el tratamiento de los datos personales realizado por las instituciones públicas. Sin embargo, más allá de la posibilidad de realizar una atenta observancia a la aplicación de la norma, no se le entregaron las facultades concretas para fiscalizar y sancionar en caso de incumplimiento.

Cabe destacar que son los organismos de la Administración del Estado, los principales tenedores de información, desempeñando un rol protagónico en el almacenamiento y registro de datos personales, entre ellos datos sensibles, necesarios para la elaboración e implementación de políticas públicas, como la entrega de beneficios, la planificación, gestión, el orden público, entre otros (Consejo, 2016:1). Al no haber delegado la Ley N°19.628 la protección de esta información a

un organismo en concreto, el Consejo debió iniciar desde su ámbito de aplicación, un proceso de educación de las instituciones públicas sobre datos personales, que hasta el momento era un tema desconocido para buena parte de los servicios.

"[En 2009] El Consejo empezó a darse cuenta que cuando se pedía información a la administración pública había una buena parte de esa información que tenía datos personales, o porque derechamente se estaban pidiendo los datos personales o porque habían datos personales de contexto que habían que proteger. Entonces, en la lógica de la transparencia uno podría decir 'todo esto es público' pero aquí hay un límite y ese límite son los derechos de las personas, bien o mal están protegidos por una ley que estamos llamados a velar." (Consejo para la Transparencia)

Así, el Consejo ha desarrollado una serie de iniciativas para informar y recomendar a los organismos del Estado la correcta aplicación de la norma, a través de diversos instructivos. El más reciente, publicado en el Compendio de Normativa Chilena Sobre Transparencia, Acceso a la Información y Protección de Datos Personales de 2015, recoge el acuerdo efectuado por el Consejo Directivo en sesión N°278, de 31 de agosto de 2011 sobre la materia .

El documento antes citado, contiene diversas recomendaciones y entrega directrices para la interpretación de la Ley N°19.628 por parte de las instituciones públicas en relación a definiciones, principios orientadores de la protección de datos, facilitación del ejercicio de los derechos de los titulares de datos personales, obligaciones específicas de los organismos de la Administración del Estado. Lo anterior, junto con aconsejar a las jefaturas de los servicios la asignación de un funcionario(a) para desempeñarse como encargado de protección de datos personales y puente de información efectivo entre el Consejo y la institución.

"[Las recomendaciones] *buscan en el fondo que la administración pública -con nuestro diagnóstico que tenía un desconocimiento desde cero, desde qué era un dato personal hasta lo que es hoy en día -al menos tienen la sensibilidad ya instalada (…) no llegan y entregan domicilios, R.U.T., correos electrónicos, que también nos pasó, o que se entregaban bases de datos completas sin tener mucha conciencia de qué era lo que significaban los datos personales de datos de origen racial, por ejemplo. Claro que cuando llegaba al Consejo ya era demasiado tarde, en especial en temas de datos personales, una vez que ya entro al flujo de los datos sin control, no lo puedes retrotraer, por mucho que digas que esto no se puede hacer".* (Consejo Para la Transparencia)

Además de la dictación de instrucciones y de proponer buenas prácticas para complementar la interpretación de la norma, el Consejo para la Transparencia resuelve en aquellos casos en que existe colisión de derechos entre la publicación de información vía Transparencia y la protección de datos por Ley N°19.628. Sobre esta materia, Jessica Matus – abogada y fundadora de la Organización Datos Protegidos- destaca *"El principio de máxima divulgación contenido en la normativa sobre transparencia y el de finalidad, en el caso de las normas sobre datos personales, ha tornado difícil el equilibrio de ambos derechos"* (Matus A., Jessica, 2013: 206).

Matus señala que si bien en las resoluciones del Consejo ha primado la reserva de información, durante la toma de decisiones se ha optado por someter las solicitudes de información a lo que se conoce como test de daño y de interés público, que en palabras de Matus (2013) se define como:

- Test de Daño: También conocido como principio de proporcionalidad, consiste en el balance entre el interés de retener la información y el interés de divulgarla para determinar si el beneficio público resultante de conocer la información solicitada es mayor que el daño que podría causar su revelación.
- Test de Interés Público: Busca determinar la existencia de un interés público que justifique la divulgación de la información o si, por el contrario, debe prevalecer su reserva para resguardar los bienes jurídicos protegidos por la ley, concretamente los derechos del tercero en cuanto a su vida privada, que serían vulnerados de publicarse la información requerida.

El desempeño que ha tenido el Consejo como órgano resolutivo cuando existe colisión de derechos en casos que involucran a instituciones públicas, ha sido criticado por algunos entrevistados, por cuanto señalan primaría en sus decisiones el interés público por sobre la protección de datos personales.

"El interés por acceso a la información e interés por la publicidad y por la data, es interés de carácter público, está en beneficio de la comunidad toda. El interés de la protección privada está en beneficio de una persona en particular, de un individuo. Entonces por lo cual gana interés público. Si aplicamos esos dos criterios a raja tabla, que es lo que hoy día ha hecho el Consejo por la Transparencia con los demás, nos encontramos con que el mismo Consejo que aplica esos criterios para efectos de resolver colisiones de bienes jurídicos en transparencia y privacidad, es el sujeto que se quiere levantar como el llamado a proteger los datos de toda la ciudadanía de nuestro país. (…) Para todos los efectos se está pidiendo que sea quien proteja la carnicería al mismo gato que está buscando efectivamente alimentarse". (Centro de Estudios en Derecho Informático)

En un mismo sentido, Carlos Reusser especialista en protección de datos destacó la labor del Consejo en materia de transparencia, no obstante, coincide en que el objetivo para el cual fue creado el organismo es distinto al que exige la protección de datos.

"El Consejo Para la Transparencia tiene una formación profesional seria que es que se preocupa y se ha preocupado siempre de la transparencia y no de la protección de datos. Su ámbito es acotado porque si tuviera que velar por la protección de datos, tendría que ser por la protección de datos de los organismos públicos, cuando se cometen abusos. Pero en el sistema privado también usan intensivamente [datos]*, no tienen tantos datos como en el sistema público, pero también usan intensivamente los datos de la gente. El Consejo Para la Transparencia, cada vez que ha habido algún conflicto entre protección de datos y transparencia, resuelve a favor de la transparencia".*

Lorena Donoso, Presidenta del Instituto de Derecho y Tecnología destaca que, si bien lo realizado hasta el momento por el Consejo responde a las escasas herramientas que desde la Ley de Transparencia se les ha entregado, se requiere realizar un cambio en la mirada al momento de resolver sobre temas vinculados a protección de datos personales.

"¿Qué puede hacer el Consejo de la Transparencia si la gente no cumple, si los organismos públicos no cumplen con las obligaciones de la Ley de Protección de Datos? Las herramientas que tienen son las que le dan la transparencia y resulta que la transparencia no es la otra cara de la moneda en protección de datos. La competencia principal del Consejo de la Transparencia, se reduce a aquellos casos en que la transparencia y la protección de datos colisionan -según ellos han entendido- sin embargo, desde nuestro punto de vista, ahí el Consejo de la Transparencia necesita un cambio de switch y darse cuenta que ellos tienen bajo su tuición dos leyes, no una sola ley interpretada de manera dicotómica, sino que son dos leyes, la Ley 19.628 y la Ley 20.575".

Otro de los ejes centrales de las críticas que realizan los entrevistados al Consejo Para la Transparencia radica en que el bien jurídico protegido en materias relacionadas a la protección de datos personales es distinto al de acceso a la información pública. Raúl Arrieta, especialista y asesor del Ministerio de Economía en el proceso de elaboración del proyecto de ley del año 2014 que buscaba modificar la norma, pone énfasis en esta dicotomía.

"En este afán de decir que la protección de datos tiene que ver con la vida privada, permanentemente se trata, se banaliza la problemática entre acceso a la información pública y protección de datos como es que son las dos caras de una misma moneda. Privacidad versus publicidad. Y la protección de datos tiene que ver con derecho fundamental y el acceso a la información pública tiene que ver con un buen gobierno, son cosas súper distintas aún cuando las dos sean de rango constitucional, en derecho."

Nicolás Yuraszeck, abogado asesor en materia de protección de datos para diversas instituciones privadas, cita el ejemplo inglés al momento de proyectar la asimilación de una autoridad que contenga bajo sus funciones velar por la protección de datos y la información pública.

"De alguna manera el sistema inglés se ha criticado por los mismos ingleses que, te tienes que ir cambiando el sombrero de acuerdo a cada situación. Por un lado protegiendo los datos personales y por otro, pidiendo acceso a la información pública. Existe evidentemente, una especie como de, rose, de disputa, tensión entre dos derechos constitucionales que parecieran ser súper buenos".

En definitiva, se considera como positivo el aporte realizado por el Consejo para la Transparencia en cuanto a abrir camino para la comprensión de la importancia de proteger los datos personales que tratan las instituciones públicas, no obstante los especialistas destacan que la experiencia de dicho organismo se centra en un aspecto concreto de la ley, quedando pendiente una supervisión más amplia que regule a las instituciones privadas y el flujo de datos transfronterizos. En este sentido, hay quienes señalan que radicar la protección de datos personales en el Consejo Para la Transparencia perjudicaría el buen trabajo que ha desempeñado este organismo como garante del acceso a la información pública.

"Si uno mira por números de base de datos de organismos públicos y privados, el Consejo para la Transparencia en más menos el 30% de los reclamos hay tensión entre protección de datos y acceso a la información pública, eso da que como el 7% de los casos que tendría que conocer este organismo corresponderían a casos de acceso de información pública. Todo el resto tendría que ver con protección de datos no relacionados con organismos públicos. Consecuentemente le podemos dar un gran abrazo del oso al Consejo de la Transparencia, o sea podemos terminar metiéndole una carga de trabajo brutal que termine por reventarlo". (Raúl Arrieta, especialista en protección de datos personales)

2. AUSENCIA DE FISCALIZACIÓN GENERA DESCONFIANZA SOBRE EL DESTINO DE LOS DATOS

Otro elemento relevante a considerar en la discusión sobre la institucionalidad en materia de protección de datos personales, guarda relación con que el tratamiento que realizan tanto las instituciones privadas como públicas carece de fiscalización, situación que impide conocer con precisión si la información está siendo utilizada para los fines que fue entregada, quiénes son responsables de su tratamiento, si se están respetando los principios de la norma, entre otros.

Algunos entrevistados señalaron que al no existir un control permanente sobre las instituciones privadas y públicas, se genera una cierta sensación de impunidad, en donde los datos personales estarían a la deriva, circulando por el mercado y expuestos a que cualquiera pueda hacer mal uso de los mismos o lucrar inclusive con información personal.

*"La filtración de datos masiva del Ministerio de Salud (…) El Ministerio le echa la culpa a Entel y Entel se lava las manos. Entel descarta responsabilidad en las fallas de seguridad informática del MINSAL que dejó expuesta la información confidencial de pacientes. O sea, ¿Cuál es la señal que uno entrega a la sociedad? Impunidad, porque estamos avalando. Aquí estamos frente a un tema donde el resultado ha sido la instauración de un marco jurídico altamente permisivo, en cuanto a las posibilidades de control que deban tener, que puedan realizar tanto los titulares de los datos, como los terceros."(*Organización de Consumidores -ODECU)

De manera similar se expresan las representantes de la Fundación Datos Protegidos, al referirse al escaso conocimiento que los usuarios poseen respecto del destino de sus datos y si la finalidad con la cual se entregó la información se ha respetado.

"IMED tiene un diseño que con la huella se está consintiendo, se está de acuerdo con que los datos van a ser almacenados, pero no que su huella se va a cruzar con otra información. Pero uno no sabe lo que pasa detrás. Porque finalmente si tú ves, ponen la base de datos en Google, en cualquier base de datos. La pasan, cruzan con el correo electrónico que por ley del consumidor y tratamiento de datos de marketing, no se le pide el consentimiento de las personas para mandar comunicaciones publicitarias" (Fundación Datos Protegidos)

Carlos Reusser, abogado y académico en derecho y tecnologías, pone énfasis en la desconfianza de los usuarios frente al sistema, la existencia de un tercero que posee información personal y que

puede determinar opciones o valoraciones del mismo en el mercado, imposibilitando o permitiendo acceder a determinados servicios.

"En la medida que vulneran los datos personales, alguien cree saber algo de ti. Y, cree estar en posición de tomar alguna decisión en tu respecto. Y tú no sabes qué es lo que saben de ti, ni a quién reclamar, ni qué verificar, ni qué corregir. Entonces a la gente le empiezan a pasar cosas. Y desde los años ochenta en adelante a la gente le pasan cosas como que no los aceptan en la ISAPRE, no los aceptan en los colegios. No les dan trabajo o cuando no les arriendan una casa donde vivir. Es decir, se ven afectados todos los derechos que tiene la Constitución, también los derechos de la ley."

Por otra parte, desde la ONG Derechos Digitales se puso énfasis en el tratamiento que actualmente se les está dando a las fuentes accesibles al público, a aquellos registros públicos o privados que al momento de generarse no requieren de autorización del titular, pero que al ser cruzado con otras fuentes proporcionan una nueva base de datos de la cual no se conoce quién es el responsable ni su finalidad.

"Entonces tu agarras la base de datos que tiene el nombre y el Rut, y otra que tiene el Rut y la dirección y otra que tiene el Rut dirección y teléfono, y otra que tiene el nombre, teléfono y, no sé, estado civil, y tú la vas estrangulando, la vas superponiendo y tú con todas las bases de datos, puedes terminar con una base de datos, que sea nombre, Rut, dirección, estado civil, correo electrónico, entonces tu al final te puedes hacer un perfilamiento perfecto. Pero como esas bases de datos no están inscritas, nadie sabe que existen y por lo tanto, tú puedes realizar esa actividad."

Desde el Servicio Nacional del Consumidor, señalan que en el desempeño de sus funciones han podido detectar una serie de falencias relacionadas con el tratamiento inadecuado de datos personales por parte de organismos privados. Esto quedaría en evidencia al momento de revisar los contratos de adhesión, particularmente en la detección de cláusulas abusivas.

"Muchas veces hay cláusulas de contrato de adhesión que dicen relación con el tratamiento de datos personales que claramente no se ajustan a los estándares que dice la ley y por ejemplo, tienen que ver con información de carácter financiero, económica y comercial de los consumidores, que no se precisan, por ejemplo cuáles son las acciones que se van a desplegar para el tratamiento (…) tampoco se precisa qué datos van a tratar, ni tampoco cuáles serán las organizaciones o entidades externas a quienes se van a ceder estos datos."

Hay quienes señalan que el débil esquema de protección de datos personales que contiene la legislación chilena, afecta a los ciudadanos de manera tal que el mal uso de información *"ha dado paso a discriminaciones arbitrarias que afectan a miles de personas a la hora de acceder al crédito y a puestos de trabajo" (Velasco y Bollier, 2016)*

Lo antes señalado, tendría relación, además, con la falta de conocimiento y comprensión de los usuarios sobre el tratamiento de datos, situación que fue señalada por los diversos participantes de la investigación.

3. ESCASA EDUCACIÓN EN PROTECCIÓN DE DATOS PERSONALES

A la desconfianza en el sistema se suma el desconocimiento tanto de la norma como de los derechos asociados. Desde las organizaciones sociales, plantean que éste sería un tema que afecta de manera transversal tanto a la ciudadanía como a las instituciones y que es posible de percibir por medio de la baja preocupación o resguardo tanto al entregar información personal como al tratarla.

Como se señaló en el acápite anterior, la inexistencia de una autoridad de control que eduque y fiscalice es indicada como una de las principales razones por las que se generaría el desconocimiento y desconfianza en el sistema. La percepción sobre una ley poco clara y un marco sancionatorio débil, son otros de los factores señalados por los participantes de la evaluación.

"Hemos advertido un bajo conocimiento de la ley y de los derechos que esta contempla por parte de los consumidores que llegan a gestionar eventualmente sus reclamos o realizan cualquier otra actividad con relación al servicio. Pero no solo bajo conocimiento de los consumidores, también de los proveedores. Este desconocimiento se traduce en distintas infracciones a la ley" (Servicio Nacional del Consumidor)

Una situación similar ha identificado el Registro Civil e identificación, mandatado por la norma para llevar el registro de banco de datos personales a cargo de las instituciones públicas. *"Durante el tiempo que este Servicio lleva el Registro, ha podido observar, por las consultas recibidas, que las personas y las instituciones tienden a confundir la naturaleza de la información que contiene este registro ya que suponen que lo que se almacena son los bancos de datos personales, propiamente tal".* (Registro Civil y de identificación en documento aportado para la investigación)

La falta de comprensión de lo que significa la entrega de información, genera además un desconcierto importante entre los usuarios de servicios, según afirman los representantes de la ONG Derechos Digitales. *"Esta sensación de que mis datos están corriendo, pero además, no tengo qué hacer al respecto y al final, esta cierta resignación de que, bueno yo entregué mis datos, bueno yo los di o los puse en internet, yo los hice públicos. Entonces está, este desazón, desconocimiento y finalmente resignación."*

En un mismo sentido, agregan desde las organizaciones de consumidores (ODECU-CONADECUS), que la falta de conocimiento genera, además, un escaso control por parte de los titulares de datos sobre la información entregada en las distintas instancias en que interactúan habitualmente. *"Pero las personas no creen, más allá del tema económico, no entienden que también el municipio tenga que resguardar mis datos de lo que estoy entregando, no entienden que el servicio electoral también puede dar mis datos cuando voy a votar. Etcétera, etcétera, y sobre todo la práctica que yo nombre recién, el tema de la huella digital. Eso es evidente, existe y punto"*.

Algunas organizaciones gremiales también se refirieron al desconocimiento como un tema que para ser mejorado necesita de una política pública de difusión, capacitación y educación. En este

sentido, consideran de alta relevancia resolver el vacío existente en la ley respecto de la definición de una autoridad de control.

"Primero que nada hay que superar un tema cultural, educacional y de valorización sobre nuestros datos personales para de alguna manera hacer mejor ejecutable cualquier ley que entre en vigencia ¿y dónde podemos encontrar esto? Justamente uno de los problemas que mencionábamos con respecto a la 19.628 es el problema de la institucionalidad. Dentro de sus funciones al igual que existen muchas otras instituciones del Estado, no solamente tiene que velar por el correcto resguardo y protección de datos personales sino que también tiene que hacer dentro de su funciones difusión, capacitación y educación". (Cámara Nacional de Comercio)

Otros entrevistados, como el especialista en protección de datos Carlos Reusser, hicieron énfasis en que entidades resolutorias en la materia, como los tribunales de justicia poseen un manejo limitado de la norma, situación que queda en evidencia en los dictámenes realizados por los jueces.

"En general es un problema, yo creo que los jueces en primera instancia no tienen los conocimientos como para resolver el asunto. O sea se resuelven en segunda instancia con los criterios que hay, pero falta de promoción del derecho, entre la población primero y a la vez a la judicatura y los operadores jurídicos en general."

Así mismo, Nicolás Yuraszeck abogado del estudio García Magliona, destaca que los jueces no están preparados en materia de datos. Si bien advierte mayor profundización en el abordaje que se da cuando los casos llegan a la Corte Suprema, en general confirma una escasa capacitación.

4. ENTIDADES PRIVADAS PONEN ÉNFASIS EN LA AUTORREGULACIÓN

Las organizaciones gremiales pertenecientes a diversos sectores participaron en dos focus group organizados por el Departamento de Evaluación de la Ley. Durante ambas jornadas dieron a conocer las medidas que han adoptado para poner en común criterios para el tratamiento de datos personales.

Así, destacaron algunos sectores que durante el periodo de vigencia de la norma han utilizado la autorregulación como mecanismo para salvaguardar el buen uso de la información, principalmente en la industria de la publicidad y el marketing. Esta opción es vista por los gremios de distintos sectores como una instancia válida que acompañada de una institucionalidad que vele por su cumplimiento, permitiría mejorar el marco de protección de los datos personales.

El representante de Asociación de Marketing Directo y Digital de Chile (AMDD) puso énfasis en su experiencia de autorregulación que la industria ha desarrollado en función de un Código que además de considerar lo normado por las leyes N°19.496 y N°19.628, toma como base el Código Chileno de Ética Publicitaria del Consejo de Autorregulación y Ética Publicitaria (CONAR).

"La industria se está autorregulando a través de un código de buenas prácticas de datos personales y otros hace ya 5 años estamos ad portas de sacar nuestro segundo código porque es un código bastante más profundo y estable. No solamente tenemos un código, si no que tenemos una certificación que nos permite certificar que los procesos estén de acuerdo con este código. (…) Nos ha costado bastante y creo que una buena ley debiera motivar y poner los incentivos correctos para que la industria se autorregule".

Otra iniciativa de autorregulación es la realizada por el Comité de Comercio Electrónico de la Cámara de Comercio de Santiago, entidad que suscribió un Código de Buenas Prácticas en el año 2014, que dedica su capítulo IV a la Protección de Datos Personales.

Por su parte la Asociación Chilena de Agencias de Publicidad (ACHAP), dio énfasis a los más de 25 años de vigencia de CONAR y destacó que cuentan con experiencia en autorregulación, señalándola como una instancia de reclamación previa a la judicialización.

Desde la Cámara de Comercio de Santiago (CCS) destacan la necesidad de introducir modificaciones a la norma en este sentido, señalando *"Creemos que sería positivo incorporar en la legislación incentivos a la autorregulación y las buenas prácticas que son fundamentales para lograr mejoras en esta materia. El comité de Comercio Electrónico de la CCS suscribió un código de buenas prácticas en el año 2014 que fue oportunamente consensuado con la autoridad pública competente".*

5. CREACIÓN DE UN ORGANISMO DE CONTROL GENERA AMPLIO CONSENSO

Existe consenso entre los entrevistados que cualquier modificación que se realice a la legislación chilena en materia de protección de datos personales debe contemplar una autoridad administrativa de control. Esta debiese ser autónoma, con capacidad sancionatoria, descentralizada y dotada de personalidad jurídica.

Desde la ONG Derechos Digitales, se pronunciaron abogando por la creación de una autoridad pública de control, en plena concordancia con legislaciones comparadas y con las exigencias de la OCDE.

"Eso es importante primero porque significaría que exista una autoridad administrativa, con capacidad sancionatoria. Pero por otro lado, porque el control sería activo y no solamente pasivo, es decir, toda vez que las personas no tienen los incentivos, las capacidades y conocimientos de que están siendo vulnerados sus derechos, o el tiempo y disposición de los recursos para judicializarlo o para llevarlo a la instancia administrativa, entonces es necesario que haya una autoridad que de oficio vele por el cumplimiento de la ley". (Organización Derechos Digitales)

Por su parte, el abogado especialista Nicolás Yuraszeck señaló la importancia de que el organismo encargado del control sea técnico y altamente capacitado, dada la especificidad de la materia. En

particular, dio cuenta de la actual falta de capacitación de los jueces, en especial de primera instancia, y del necesario cambio que debe tener lugar hacia un procedimiento administrativo.

"El tema de la institucionalidad se tiene que ver por un órgano técnico, administrativo, autónomo, con dedicación exclusiva, obviamente con profesionales altamente capacitados y también para poder lograr todo esto tenemos que tener un procedimiento especial. Un procedimiento especial administrativo. No podemos estar, hoy por hoy, metiendo al saco del aspecto judicial todo esto".

Desde las organizaciones gremiales destacaron la importancia de que este nuevo órgano contara con profesionales técnicos que, adicionalmente, certificaran los códigos de buenas prácticas e iniciativas de autorregulación.

"Es fundamental que este Consejo sea autónomo e independiente, y en el fondo para eso que es un punto clave, creemos que ayudaría mucho tener profesionales. Que los miembros del Consejo sean profesionales, expertos en materia de protección de datos y tengan dedicación exclusiva. Creemos también que sería conveniente que la legislación incorporara incentivos a la autorregulación, a los códigos de buenas prácticas y que este mismo consejo de repente certifique esos códigos."

El carácter técnico de este organismo, fue también abordado por Raúl Arrieta, asesor legal del Ministerio de Economía durante el proceso de elaboración del proyecto de Ley en el año 2014. Durante ese periodo, se desarrollaron mesas de diálogo que contaron con una amplia participación de actores de diversos sectores. En ese contexto, se generaron una serie de consensos, donde la institucionalidad fue un punto relevante en la discusión.

"Y les encantó el diseño institucional que se había logrado, que era un organismo colegiado con un presidente designado por el Presidente de la República de una quina propuesta por la Corte Suprema, con título de abogado y creo que eran 15 años de experiencia. Era algo parecido al mecanismo de nombramiento del presidente del tribunal de defensa de libre competencia. Y después tienes a 4 consejeros más, 2 abogados y 2 no abogados. Un abogado y un no abogado propuestos por el ejecutivo y ratificados por el senado y los otros dos propuestos por la Corte Suprema".

Es importante señalar, que la visión mayoritaria de los entrevistados destacó la necesidad de un ente autónomo con dedicación exclusiva, descartando la nominación del Consejo para la Transparencia como organismo regulador de la protección de datos personales.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

La promulgación de la Ley N°19.628 se constituyó como un avance en la regulación del tratamiento de datos personales a finales de los años noventa. Sin embargo, a 17 años de su entrada en vigencia, la norma no se ajusta al rápido y masivo flujo de información que el actual desarrollo tecnológico exige.

Existe consenso entre los entrevistados sobre la necesidad de hacer una reforma a la legislación de protección de datos que permita brindar mayores garantías para los titulares sobre el destino de su información y una normativa más clara con mayor certeza jurídica para quienes los tratan.

Por su parte, la Organización para la Cooperación y el Desarrollo Económicos (OCDE) ha reiterado la conveniencia de que nuestro país cuente con un marco normativo más sólido, solicitando al Estado de Chile el cumplimiento del compromiso adquirido al momento de ingresar a dicho organismo.

Diversos han sido los intentos efectuados por el Poder Ejecutivo y Legislativo para modificar la norma. Una consulta pública y un número importante de mesas de diálogo integrada por actores provenientes del mundo académico y empresarial forman parte de un largo recorrido que, desde la perspectiva de los entrevistados, no ha entregado resultados concretos.

A continuación se exponen las principales conclusiones y recomendaciones obtenidas de la Evaluación de la Ley N°19.628.

ÁMBITO DE APLICACIÓN CARECE DE PRECISIÓN

La Ley N°19.628, en su artículo primero, regula el tratamiento de los datos de carácter personal, tanto por organismos públicos, privados y particulares, a excepción del que se efectúe en ejercicio de las libertades de emitir opinión e informar.

Asimismo, la Ley permite el tratamiento de datos personales siempre que se haga de manera concordante con ésta y para finalidades permitidas por el ordenamiento jurídico. Del mismo modo, consagra el respeto que debe existir por parte de quienes tratan datos al pleno ejercicio de los derechos fundamentales de los titulares y a las facultades que la norma les reconoce.

Cabe destacar que la ley no contempla como excepción a su aplicación el tratamiento de datos personales de carácter doméstico, o aquel que debe realizarse como parte de la ejecución de un contrato de carácter laboral. Por otra parte, tampoco regula aquellas hipótesis en que prestadores de servicios globales se encuentran fuera del país prestando servicios a personas dentro de Chile.

Se recomienda:

- Precisar las normas sobre el ámbito de aplicación, exceptuando ciertos tratamientos de datos personales como aquellos de carácter doméstico.
- Establecer en la Ley que esta se aplica respecto de servicios prestados en Chile aunque el prestador no se encuentre en el país.

CONCEPTO DE DATO PERSONAL ES INSUFICIENTE

La Ley define dato personal como aquel relativo a cualquier información concerniente a personas naturales, identificadas o identificables. Respecto a este concepto, se criticó que no entregaría suficientes elementos para establecer si un dato es personal o no lo es y el límite entre un dato personal y un dato estadístico (aquel que no puede ser asociado a un titular identificado o identificable). Asimismo, existe complejidad al momento de dotar de contenido al concepto de *persona identificable*.

Se recomienda:

- Perfeccionar los conceptos de dato personal y dato estadístico, consagrando elementos que permitan distinguir de mejor manera uno y otro.
- Clarificar el concepto de *persona identificable.*

ACTORES QUE INTERVIENEN EN EL TRATAMIENTO DE DATOS NO SON CONSIDERADOS POR LA NORMA

El artículo 2° define figura responsable de registro o banco de datos como "*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*".

Respecto a esta materia, se señaló que actualmente existe un vacío en relación a la distinción entre los diversos actores que intervienen en los procesos de tratamiento de datos personales y sus roles y responsabilidades en tales calidades. Esta distinción sería necesaria considerando que existen múltiples etapas en el tratamiento de la información, en las cuales intervienen una pluralidad de actores.

Se recomienda:

- Perfeccionar el concepto de responsable de banco de datos e incorporar en la Ley los conceptos de controlador, encargado, intermediario o procesador, consagrando deberes y obligaciones cuyo incumplimiento lleve aparejada una sanción.

REGULACIÓN DEL CONSENTIMIENTO NO CONTEMPLA NUEVAS TECNOLOGÍAS

El artículo 4° de la Ley N° 19.628 permite el tratamiento de los datos personales y lo considera lícito únicamente cuando dicha norma u otras disposiciones legales lo autoricen o en caso que el titular consienta expresamente.

De este modo, la legitimidad del tratamiento de datos está condicionada a la autorización del titular de los datos, a menos que exista una norma legal que exima de esta autorización.

Actualmente, el consentimiento se regula respecto de todos los tipos de datos sin distinción, lo que fue criticado por expertos debido a que no contemplaría mayores exigencias para datos de mayor relevancia como aquellos sensibles. Por otra parte, no queda claro el cumplimiento de la exigencia de escrituración del consentimiento en caso de que este se otorgue a través de sistemas informáticos, situación que contribuye a una incerteza jurídica.

Se recomienda:

- Distinguir en la Ley tipos de consentimiento dependiendo de la clase de dato que se trate: En particular, respecto a los datos sensibles, consagrar un consentimiento expreso y previo. Para otro tipo de datos, analizar la incorporación de un consentimiento inequívoco y no necesariamente previo.
- Incorporar en la Ley el deber y responsabilidad de quien realiza la operación de tratamiento de datos de establecer mecanismos que permitan a los titulares dar un consentimiento inequívoco y suficientemente informado.
- Explicitar en la Ley si un consentimiento otorgado a través de tecnologías informáticas satisface el requisito de escrituración.

EXCEPCIONES SE CONVIERTEN EN REGLA GENERAL

La Ley N°19.628 permite el tratamiento de datos personales sin requerir el consentimiento de su titular en una serie de situaciones, la mayoría contenidas en el artículo 4° y dos en los artículos 10° y 20°. Estas son aquellos obtenidos de fuentes accesibles al público, el tratamiento efectuado por personas jurídicas privadas en ciertos casos, aquel realizado por organismos públicos y los datos sensibles con relación a beneficios de salud.

Estas normas fueron criticadas por los expertos e implementadores entrevistados, debido a su amplitud, lo que dejaría el principio del consentimiento con poca utilización y lo convertirían en la excepción.

FUENTES ACCESIBLES AL PÚBLICO: DEFINICIÓN POCO CLARA Y ESCASO CONTROL SOBRE SU FINALIDAD

La Ley define fuentes accesibles al público, como aquellos "*registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes*". Este concepto fue cuestionado debido a su amplitud y por el hecho de radicar en manos del titular del registro la facultad de dejarlo o no abierto al público, especialmente considerando el escaso conocimiento detectado sobre la materia. Del mismo modo, se estimó que este concepto no se encuentra estructurado de una forma que permita proteger los datos personales.

Por otra parte, la excepción de fuente accesible al público fue criticada debido a que su redacción no es clara, ya que no precisa si esta excepción al consentimiento opera respecto de ciertos datos obtenidos a través de este tipo de fuentes o si dicho concepto es una excepción en sí misma.

En este sentido, el artículo 4° inciso 5° dispone *"No requiere autorización el tratamiento de datos que provengan o se recolecten de fuentes accesibles al público, cuando sean de carácter económico, financiero, bancario o comercial, 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 sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios".*

De este modo, subsiste la discusión interpretativa que dificulta la aplicación uniforme del derecho tanto para titulares como para quienes tratan datos.

Finalmente, fue criticada por la ausencia de un requisito de respeto a la finalidad en el tratamiento de los datos personales obtenidos por dichas fuentes. Esta situación ha generado que existan cruces de bases de datos obtenidos de este tipo de fuentes sin ningún control.

Se recomienda:

- Consagrar en la Ley de forma taxativa aquellas fuentes que revisten el carácter de accesibles al público, a través de un listado cerrado, para efectos de la normativa de protección de datos.
- Clarificar que la excepción de fuentes accesibles al público sólo opera respecto de cierto tipo de datos y no como excepción en sí misma.
- Incorporar en la normativa el necesario respeto al principio de finalidad, contemplando sanciones en caso de su vulneración.

IMPRECISIÓN EN EL TRATAMIENTO DE DATOS POR PERSONAS JURÍDICAS PRIVADAS

El artículo 4° señala que tampoco requiere de 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*".

Fue criticada esta excepción por la complejidad interpretativa de su redacción y su falta de contenido concreto. Lo anterior genera diferencias en su aplicación, dando pie para una utilización abusiva.

Se recomienda:

- Clarificar de forma más detallada casos en los cuales es posible hacer uso de esta excepción al consentimiento para las personas jurídicas privadas.

UTILIZACIÓN ABUSIVA DE DATOS SENSIBLES

La Ley define dato sensible como aquel que se refiere "*a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual*".

En este sentido, se aprecia como positivo que el concepto de dato sensible sea de carácter abierto, sin embargo, se señaló que no contiene suficientes ejemplos respecto de los cuales se permita calificar como indudable su calidad de sensible. Del mismo modo, hubo consenso en que la normativa actual no brinda protección suficiente a este tipo de datos.

En relación a su tratamiento como excepción, el artículo 10 de la norma prohíbe de forma general el tratamiento de 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.

Cabe señalar que las dos primeras excepciones son comunes a todos los tipos de datos, por lo que la particularidad se da en permitir el tratamiento de datos sensibles sin consentimiento del titular cuando sean necesarios para el otorgamiento de beneficios de salud.

Esta excepción fue criticada por los expertos, alegando un abuso por parte de los actores de la industria de salud que la utilizan fuera de la intención del legislador, la cual habría sido consagrarla para efectos del copago.

Se recomienda:

- Perfeccionar el concepto de dato sensible incorporando como criterio principal la posibilidad de eventuales discriminaciones en base a esos datos.
- Incorporar dentro del concepto de datos sensibles los datos referentes a menores de edad.
- Regular de forma más estricta el tratamiento de datos sensibles, con un estándar de consentimiento expreso, incorporando obligaciones especiales de información, conservación, seguridad y revisión de comunicación a terceros, y sanciones más gravosas.
- Clarificar en la Ley el alcance y contenido de la frase "beneficios de salud", estableciendo parámetros para su uso.

AUSENCIA DE LÍMITES EN EL TRATAMIENTO DE DATOS POR ORGANISMOS PÚBLICOS

El artículo 20° dispone que los organismos públicos sólo podrán tratar datos personales respecto de las materias de su competencia y con sujeción a la norma. En esas condiciones, no necesita el consentimiento del titular.

Se criticó esta norma debido a la extensión de facultades que se confieren, lo que constituye una importante excepción al consentimiento, en especial considerando la relevancia que adquiere el Estado como procesador y recolector de datos personales.

Se recomienda:

- Clarificar que la omisión a la autorización del titular opera sujeta al principio de finalidad y manteniendo las dos condiciones señaladas en el artículo 20°.

REGISTRO DE BANCO DE DATOS DE ORGANISMOS PÚBLICOS

El artículo 22° de la Ley dispone la creación de un registro de bancos de datos personales a cargo de organismos públicos por parte del Servicio de Registro Civil e Identificación. Asimismo, dispone su carácter público y que en el debe constar el fundamento jurídico de la existencia del banco de datos, su finalidad, tipos de datos almacenados y descripción del universo de personas que comprende.

A su vez, consagra la obligación del organismo público de proporcionar los antecedentes al Servicio cuando se inicien actividades y comunicar cualquier cambio de los elementos indicados. Sin embargo, el Servicio de Registro Civil informó que a mayo de 2016, sólo 99 organismos públicos han informado respecto de los bancos de datos personales a su cargo. Lo anterior, de un universo estimado de aproximadamente 700 organismos que se encontrarían dentro del ámbito de aplicación de la norma. A mayor abundamiento, indica a modo de ejemplo, que de las cerca de las 344 Municipalidades del país, sólo 5 han dado cumplimiento a la norma.

Esto da cuenta de una limitada aplicación del artículo 22° y de la falta de incentivos legales que hagan posible un cumplimiento por parte del sector público.

Se recomienda:

- Incorporar en la Ley una sanción para aquellos organismos públicos que no inscriban sus bases de datos en el Registro Civil, de acuerdo a lo dispuesto en el artículo 22° de la Ley, en un plazo determinado.

PROCEDIMIENTO DE AMPARO: INDEFENSIÓN DEL AFECTADO POR INFRACCIONES A LA LEY

El artículo 16° de la Ley N°19.628 consagra un procedimiento de amparo a los derechos consagrados de información, modificación, eliminación y bloqueo, el cual tiene lugar cuando el responsable del registro no se pronuncia sobre la solicitud de dichos derechos o la deniega por causa distinta de la seguridad o interés nacional.

En este caso, el titular de los datos tiene derecho a recurrir al juez de letras en lo civil del domicilio del responsable. Esto configura la principal crítica del procedimiento, ya que implica un costo para el afectado y un tiempo de tramitación considerable que no se ajusta a las exigencias de los actuales sistemas de información.

Se recomienda:

- Trasladar este procedimiento a la autoridad administrativa de control que se defina, manteniendo como segunda instancia la Corte de Apelaciones.
- Contemplar procedimiento sancionatorio a cargo de una autoridad de control con facultades para instruirlo y aplicar las sanciones.

NORMA CARECE DE SANCIONES EFECTIVAS EN CASO DE INFRACCIÓN

El artículo 16° señala las sanciones que puede imponer el juez en caso de acogerse la reclamación, disponiendo multas que van de 1 a 50 unidades tributarias mensuales.

Con relación a esta materia, fue altamente criticada la inexistencia de un régimen completo de infracciones y sanciones en la Ley, así como también la baja cuantía de las multas actuales. Del mismo modo, también se cuestionó la ausencia de sanciones para aquellas entidades públicas o privadas que sufren una fuga de datos y no dan aviso a los titulares afectados.

Cabe destacar que la ausencia de una autoridad de control y de un procedimiento de reclamación expedito, incide directamente en la impunidad de quienes infringen la ley.

Se recomienda:

- Incorporar un catálogo completo de infracciones con sus correspondientes sanciones de una cuantía que se pueda graduar de acuerdo a la gravedad de éstas.

- Incluir incentivos para comunicar a los titulares cuando tenga lugar alguna fuga de datos.
- Consagrar en la Ley deberes y obligaciones diferenciados para quienes tratan datos dependiendo de la calidad de estos.

FISCALIZACIÓN Y CONTROL: AUSENCIA DE ÓRGANO ADMINISTRATIVO REPERCUTE EN LA APLICACIÓN DE LA NORMA

El texto legal que regula el tratamiento de datos personales en Chile no hace referencia explícita entre sus articulados a una institución que vele por el cumplimiento de la norma. La ausencia de un organismo que eduque, controle y fiscalice la protección de datos personales con un alcance transversal a todos los actores que tratan información de estas características, es indicada como una de las principales debilidades de la norma en Evaluación.

En ese contexto, el Consejo para la Transparencia debió asumir la labor de velar por el cumplimiento de la norma por parte de los organismos públicos, en cumplimiento del mandato de la Ley N°20.285 que dispuso su creación.

Si bien los entrevistados destacaron su rol en cuanto a la difusión de la norma y las recomendaciones que el Consejo ha realizado sobre su aplicación, enfatizaron que su alcance ha sido limitado debido a que este no posee facultad fiscalizadora ni sancionatoria.

Así mismo, se cuestionaron los criterios con los que el Consejo para la Transparencia ha resuelto en casos en que se ha producido colisión de derechos entre acceso a la información y protección de datos, visión que descartaría la nominación de este organismo como ente regulador de la protección de datos personales.

Por otra parte, el tratamiento que realizan tanto las instituciones privadas como públicas carece de fiscalización, situación que impide conocer con precisión, por ejemplo, si la información está siendo utilizada para los fines que fue entregada, quiénes son responsables de su tratamiento o si se están respetando los principios de la norma.

La inexistencia de un control permanente sobre quienes tratan datos genera, además, desconfianza sobre el destino de la información, dando pie para un uso inadecuado de la misma, el que en opinión de entrevistados puede materializarse en limitantes para acceder a un crédito u opción laboral, la imposibilidad de distinguir cláusulas abusivas, entre otros.

A la desconfianza en el sistema se suma el desconocimiento tanto de la norma como de los derechos asociados. Desde las organizaciones sociales, plantean que éste sería un tema que afecta de manera transversal tanto a la ciudadanía como a las instituciones y que es posible de percibir por medio de la baja preocupación o resguardo tanto al entregar información personal como al tratarla. Este desconocimiento también se proyecta en los tribunales de justicia quienes poseerían un manejo limitado de la norma.

En definitiva, existe consenso entre los entrevistados que la legislación chilena en protección de datos personales requiere de una autoridad administrativa de control independiente, que facilite el acceso tanto de los titulares como de los responsables de datos a un procedimiento expedito no judicializado.

Se recomienda:

- Establecer la creación de una autoridad administrativa con capacidad sancionatoria, autonomía y patrimonio propio.
- Generar una fiscalización permanente y de oficio por parte de esta autoridad.
- Facultar a esta autoridad para certificar códigos de autorregulación de las distintas industrias.
- Elaborar una política pública de difusión, capacitación y educación en protección de datos personales.

CAPÍTULO VI. BIBLIOGRAFÍA

Cerda, Alberto (2012). Legislación sobre protección de las personas frente al tratamiento de datos personales., Material de Estudio Centro de Estudios en Derecho Informático, Facultad de Derecho Universidad de Chile.

Consejo Para la Transparencia. (2015). Compendio de normativa chilena sobre transparencia, acceso a la información y protección de datos personales. Leyes y reglamentos. Instrucciones, recomendaciones y acuerdos del Consejo para la Transparencia. Santiago, Chile.

CORFO (Corporación de Fomento de la Producción) (2009) *Balance Consejo Estratégico del Cluster de Servicios Globales*. Disponible en: http://www.corfo.cl/downloadfile.aspx?CodSistema=20020129172812&CodContenido=20091023174703&CodArchivo=20091023175059

DE TERWANGNE, Cécile (2012). Privacidad en Internet y el derecho a ser olvidado/derecho al olvido. En VII Congreso Internacional Internet, Derecho y Política. Neutralidad de la red y otros retos para el futuro de Internet. IDP. Revista de Internet, Derecho y Política. N.º 13, pág. 53-66. http://idp.uoc.edu/ojs/index.php/idp/article/view/n13-terwangne_esp/n13- terwangne_esp

Hafner y Wilkins (2014). El "derecho al olvido" en el espacio virtual, Derecho nacional y comparado. Asesoría Técnica Parlamentaria, Biblioteca del Congreso Nacional. https://www.bcn.cl/asesoriasparlamentarias/buscar?texto=El+%E2%80%9Cderecho+al+olvido%E2%80%9D+en+el+espacio+virtual.+Derecho+nacional+y+comparado

Informe del Comité Jurídico Interamericano de la Organización de los Estados Americanos, Privacidad y Protección de Datos Personales. 86° Periodo Ordinario de Sesiones 23-27 de marzo de 2015. Rio de Janeiro, Brasil. Disponible en http://www.oas.org/es/sla/ddi/docs/CJI-doc_474-15_rev2.pdf

Matus Arenas, Jessica. Derecho de acceso a la información pública y protección de datos personales. Revista Chilena de Derecho y Tecnología. Centro de Estudios en Derecho Informático, Universidad de Chile. Vol.2 Núm. 1(2013).Págs. 197-228

Mieres, L. J. (2014). *El derecho al olvido digital.* Fundación Alternativas: http://www.fundacionalternativas.org/public/storage/laboratorio_documentos_archivos/e0d97e985163d78a27d6d7c23366767a.pdf

Ministerio de Economía Fomento y Turismo (2014). *Documento de Respuesta Consulta Ciudadana Anteproyecto Ley Protección de las Personas del Tratamiento de Datos Personales.* Disponible en:

http://www.participacionciudadana.economia.gob.cl/sites/default/files/2014-10-21%20Respuesta%20Consulta%20Ciudadana_0.pdf

Tribunal de Justicia de la Unión Europea. Sentencia del Tribunal de Justicia en fallo "Costeja con Google Inc." del 13 de mayo de 2014. http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES

The Boston Consulting Group (2007). *Estudios de Competitividad en Clusters de la Economía Chilena. Informe final.* Disponible en http://www.economia.gob.cl/1540/articles-187159_recurso_1.pdf

a. Normativa Internacional

Consejo de Europeo. Reglamento general de Protección de Datos. http://www.consilium.europa.eu/es/policies/data-protection-reform/data-protection-regulation/

Convención Americana sobre Derechos Humanos. (Pacto de San José). San José, Costa Rica 7 al 22 de noviembre de 1969. http://www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos.htm

Convenio 108 del Consejo de Europa, de 28-1-1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981. https://www.coe.int/t/dghl/standardsetting/dataprotection/Global_standard/Conv%20108_es.pdf

Corporación Económica Asia – Pacífico. (2005). Marco de Privacidad del Foro de Cooperación Económica Asia Pacífico. (APEC). Singapur. https://www.sellosdeconfianza.org.mx/docs/marco_de_privacidad_APEC.pdf

Declaración Americana de Derechos y Deberes del Hombre. Bogotá, Colombia, 1948. https://www.oas.org/dil/esp/Declaraci%C3%B3n_Americana_de_los_Derechos_y_Deberes_del_Hombre_1948.pdf

Declaración Universal de Derechos Humanos. http://www.un.org/es/documents/udhr/

Directiva 95/46/CE del parlamento europeo y del consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:31995L0046

Directrices para la Regulación de los Archivos de Datos Personales Informatizados, adoptadas mediante la resolución 45/95 de la Asamblea General de la Organización de las Naciones Unidas. http://www.un.org/es/documents/ag/res/45/list45.htm

Estándares Internacionales sobre Protección de Datos Personales y Privacidad,. Resolución de Madrid. 31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad. https://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_es.pdf

Organización para la Cooperación y el Desarrollo Económicos. (1980). Directrices relativas a la Protección de la intimidad y de la circulación transfronteriza de datos Personales. http://inicio.ifai.org.mx/Estudios/OCDE-Directrices-sobre-protecci-oo-n-de-privacidad-Trad.pdf.pdf

Organización para la Cooperación y el Desarrollo Económicos. (2002). Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales. http://www.oecd.org/sti/ieconomy/15590267.pdf

Organización para la Cooperación y el Desarrollo Económicos. Declaración Ministerial relativa a la Protección de la Intimidad en las Redes Globales. Ottawa 7-9 octubre de 1998 http://www.oas.org/es/sla/ddi/docs/Declaracion_OCDE_Proteccion_Intimidad_redes.pdf

Organización para la Cooperación y el Desarrollo Económicos. (2013). Marco de Privacidad de la Organización para la Cooperación y el Desarrollo Económicos. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

Resolución A/C.3/68/L.45/Rev.1, "El derecho a la privacidad en la era digital" aprobada por la Asamblea General de la Organización de las Naciones Unidas. https://documents-dds-ny.un.org/doc/UNDOC/LTD/N13/576/80/PDF/N1357680.pdf?OpenElement

Pacto Internacional de Derechos Civiles y Políticos. 16 de diciembre de 1966. http://www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx

Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES

Resolución AG/RES. 2842, Acceso a la información pública y protección de datos personales aprobada por la Asamblea General de la Organización de los Estados Americanos. http://www.oas.org/es/sla/ddi/docs/AG-RES_2842_XLIV-O-14.pdf

b. Legislación Extranjera:

Agencia Española de Protección de Datos. http://www.agpd.es/portalwebAGPD/index-ides-idphp.php

Consejo para la Transparencia. Plataforma del curso protección de datos personales. http://www.educatransparencia.cl/abiertos/proteccion_datos/

Constitución Española de 1978. http://www.lamoncloa.gob.es/documents/constitucion_es1.pdf

Constitución de la República Oriental del Uruguay de 1967. https://www.presidencia.gub.uy/normativa/constitucion-de-la-republica

Instituto nacional de Estadísticas de la República Oriental del Uruguay. http://www.ine.gub.uy/
Ley N°19.628 sobre la Protección de la Vida Privada. https://www.leychile.cl/Navegar?idNorma=141599

Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD). https://www.boe.es/buscar/doc.php?id=BOE-A-1992-24189

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/common/pdfs/2014/Ley_Organica_15-1999_de_13_de_diciembre_de_Proteccion_de_Datos_Consolidado.pdf

Ley N° 18.331, de 11 de agosto de 2008 sobre Protección de Datos Personales y Acción de "Habeas Data". http://www.agesic.gub.uy/innovaportal/v/302/1/agesic/ley-n%C2%B0-18331-de-11-de-agosto-de-2008.html

Unidad Reguladora y de Control de Datos Personales. https://datospersonales.gub.uy/inicio/

www.evaluaciondelaley.cl / / Teléfono: (32) 2505424 / email: evaluaciondelaley@congreso.cl

Diseño y Publicaciones
Cámara de Diputados de Chile