SERIE DE
DOCUMENTOS
MATERIALES
DOCENTES

ACADEMIA
JUDICIAL
CHILE

Protección de Datos Personales

Autores

Lorena
Donoso
Abarca

Carlos
Reusser
Monsálvez

Academia Judicial de Chile | www.academiajudicial.cl

SERIE DE
DOCUMENTOS
MATERIALES
DOCENTES

ACADEMIA JUDICIAL CHILE

Autores

Lorena Donoso Abarca

Abogada de la Universidad de Chile, es Magíster en Informática y Derecho por la Universidad Complutense de Madrid. Árbitra de NIC Chile para la resolución de conflictos sobre nombres de dominio en internet, también es consejera del Instituto Chileno de Derecho y Tecnologías y profesora asociada del Departamento de Derecho Procesal de la Universidad de Chile. Fue directora del Centro de Estudios en Derecho Informático de esa misma universidad.

Carlos Reusser Monsálvez

Abogado de la Universidad de Chile y Magíster en Derecho Constitucional por la Pontificia Universidad Católica de Chile, es Máster en Informática y Derecho y Especialista en Derechos Humanos por la Universidad Complutense de Madrid. Experto en Gestión del Conocimiento por la Universidad Carlos III de Madrid, es profesor de Derecho de la Información en la Universidad Alberto Hurtado y consejero del Instituto Chile- no de Derecho y Tecnologías.

Academia
Judicial
de Chile

Diseño y
Diagramación:
Estudio Real
somosreal.cl

Material
docente N° 32

Santiago,
Chile 2021

ISBN N°
2022-A-1850

Resumen

Bajo el concepto *protección de datos personales* se engloba un conjunto de principios y normas relativas a la recolección, almacenamiento, análisis y comunicación de información referida a personas naturales, que se ha venido desarrollando en los sistemas jurídicos de derecho continental europeo desde 1983 en adelante cuyo fin no es otro que el de evitar la vulneración de los derechos fundamentales de las personas a través del tratamiento abusivo de sus propios datos.

Nuestro país no es ajeno a esta realidad y ya en 1999, a través de la Ley Nº 19.628, persiguió este mismo objetivo, aunque hoy se encuentra en un necesario proceso de revisión dado que su texto legal ha sido superado por el desarrollo tecnológico y los estándares internacionales aplicables en la materia.

De la regulación de aquel entonces y sus motivaciones, así como de las directrices actuales y futuras de este nuevo derecho fundamental, damos detallada cuenta en el presente curso.

Palabras clave

Protección de datos – datos personales – autodeterminación informativa – derechos fundamentales – seguridad de datos.

Índice de contenidos

Tabla de abreviaturas 7

Introducción 8

1. La problemática de la protección de datos personales 10

1.1 Antecedentes históricos del derecho fundamental a la protección de datos 11

1.2 El precedente: la *Privacy* norteamericana 12

1.3 La vía europea principal: la intimidad 16

1.4 El aporte alemán: derecho a la autodeterminación informativa 18

1.5 La autodeterminación informativa y su recogida en Chile 22

1.6 Conceptos esenciales: datos, banco de datos, tratamiento y responsables 27

1.7 Categorías de datos personales y sus implicancias desde la óptica de su protección 32

2. Estándares internacionales de protección de datos personales 38

2.1 La protección de datos en Europa 39

2.1.1 Convenio Nº 108 del Consejo de Europa, de 28 de enero de 1981 42

2.1.2 El determinante fallo del Tribunal Constitucional Alemán en el caso de la Ley del Censo de 1983 45

2.1.3 Directiva 95/46/CE, del Parlamento Europeo y del Consejo de 24 de octubre de 1995 51

2.1.4 Reglamento General de Protección de Datos (RGPD), de 25 de mayo de 2018, como estándar de facto para la interpretación de la protección de datos personales en Chile 54

2.2 Estándares de protección de datos personales de la OCDE (2002) 57

2.3 Principios en materia de protección de datos personales en la Resolución de Madrid (2009) 60

2.4 Estándares de protección de datos personales para los Estados iberoamericanos (OEA, 2016) 66

2.5 Acuerdo de Asociación entre la Comunidad Europea y Chile y sus efectos en materia de protección de datos personales 69

3. El desarrollo normativo de la protección de datos en Chile 72

3.1 La reforma constitucional de 2018 73

3.2 La Ley Nº 19.628 de 1999 y sus modificaciones 78

3.3 La protección de datos y las leyes procesales 88

3.4 Las políticas judiciales en materia de protección de datos personales 92

3.5 Acción de ***habeas data*** y su aplicación práctica en Chile 100

3.6 El régimen infraccional en la Ley Nº 19.268 108

4. Principios y derechos en materia de tratamiento de datos personales. Análisis desde la doctrina y la jurisprudencia. 110

4.1 Principio de lealtad y licitud del tratamiento de datos 111

4.2 Principio general de legitimación 112

4.2.1 El consentimiento del interesado 112

4.2.2 La autorización legal como legitimante 114

4.2.3 El interés legítimo como "legitimante" 118

4.3 Principio de transparencia (información y publicidad) 123

4.3.1 Deber de notificación y Registro 123

4.3.2 Deber de información 124

4.4 Principio de finalidad 129

4.5 Principio de calidad 131

4.5.1 Condiciones relativas a la calidad de los datos personales 131

4.5.2 Proporcionalidad 136

4.5.3 Temporalidad del tratamiento 138

4.5.4 Calidad de proceso 139

4.5.5 Cumplimiento de derechos de los titulares de datos 139

4.6 Principio de control 141

5. Deberes legales especialmente exigibles 144

5.1 Deber de seguridad en el tratamiento de datos personales 145

5.2 Protección de datos desde el diseño 149

5.2.1 Proactivo, no reactivo ni remedial 152

5.2.2 Privacidad como configuración determinada o por defecto 152

5.3 Evaluaciones de impacto y consulta previa 158

5.4 Responsabilidad demostrada 162

5.5 Enfoque de riesgos y gestión de seguridad de los datos personales 163

6. Los derechos de los titulares de datos frente a la doctrina y jurisprudencia 166

6.1 Derecho de acceso 167

6.2 Derecho de rectificación 169

6.3 Derecho de cancelación o supresión 170

6.4 Derecho de oposición 171

6.5 Cambios en el ámbito de los derechos a partir de la entrada en vigencia del RGPD 173

6.6 Aplicación del derecho de cancelación a internet: el "derecho al olvido" 175

7. Eventuales modificaciones a la normativa vigente y su impacto en el control judicial. La situación actual y los cambios que se debaten. 194

7.1 Autoridades de control 195

7.2 El nuevo derecho a la portabilidad de los datos 198

7.3 Notificación de vulneraciones de seguridad 199

7.4 Régimen infraccional 201

8. El tratamiento de datos por el Estado 203

8.1 Legitimación para el tratamiento de datos 204

8.2 El tratamiento de datos por los organismos de inteligencia y seguridad 207

8.2.1 Policía de Investigaciones 207

8.2.2 Carabineros de Chile 208

8.2.3 Agencia Nacional de Inteligencia 209

8.2.4 Protección de datos y actividades de videovigilancia para la mantención de la seguridad pública 210

8.3 Autorización para realizar tratamiento de datos personales por otros organismos públicos 216

8.3.1 Defensoría de la Niñez 216

8.3.2 Instituto Nacional de Derechos Humanos 217

8.3.3 Servicio Electoral 218

8.4 Tratamiento de datos personales y la prueba en juicio 219

8.4.1 Tratamiento de datos de imágenes y video para preconstitución de pruebas en juicios civiles 219

8.4.2 Tratamiento de datos de videovigilancia como prueba en los juicios laborales 220

9. Desafíos de la protección de datos en el tránsito a la automatización 224

9.1 El fenómeno de la minería de datos y el big data y las formas de control judicial 225

9.2 El "targeting", los algoritmos y la predicción de consumo 230

9.3 Internet de las cosas (IoT) y tratamiento de datos personales 234

9.4 Videovigilancia e imágenes como datos personales 239

9.5 Datos en internet y redes sociales 241

Tabla de abreviaturas

AEPD:	Agencia Española de Protección de Datos (personales)
CNIL:	Comisión Nacional de la Informática y las Libertades (Francia)
OCDE:	Organización para la Cooperación y el Desarrollo Económico
ONU:	Organización de las Naciones Unidas
RGPD:	Reglamento General de Protección de Datos de Europa
RIPD:	Red Iberoamericana de Protección de Datos
TJUE:	Tribunal de Justicia de la Unión Europea
SUSESO:	Superintendencia de Seguridad Social
TCCh:	Tribunal Constitucional de Chile
TCA:	Tribunal Constitucional de Alemania
TCE:	Tribunal Constitucional de España

Introducción

Bajo el concepto *protección de datos personales* se engloba un conjunto de normas y principios relativos a la recolección, almacenamiento, análisis y comunicación de información relativa a personas naturales, el que tiene como fin último que no se vulneren los derechos fundamentales de las personas con ocasión del tratamiento de la misma.

Con el desarrollo de las tecnologías de la información y las comunicaciones (TIC) y su aplicación a prácticamente todas las esferas de la sociedad, estas actividades de tratamiento de datos se han masificado y también sofisticado al punto que ya no es necesario solicitar a la propia persona que entregue información que le concierne, sino que los motores de búsqueda y algoritmos computacionales que se comportan como robots (*bots*), además de múltiples sensores instalados en cosas y en espacios públicos y privados, van recolectando información de las personas.

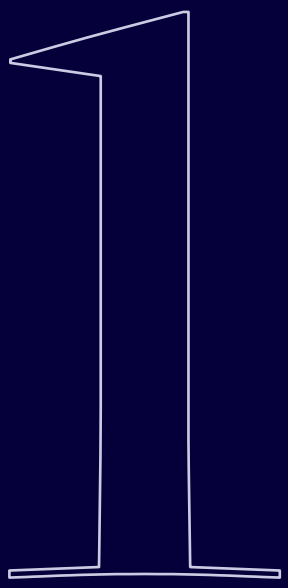
Luego, a través de algoritmos de procesamiento y en base a los datos recolectados, se hace posible predecir el comportamiento de esa persona o de su entorno y, más todavía, provocar estímulos para conseguir determinados resultados.

Mediante este curso no se pretende que el estudiante adquiera conocimientos técnicos acerca del funcionamiento de los algoritmos de procesamiento de datos, sino más bien que se aproxime a la preocupación existente en torno al tema y comprenda el razonamiento que subyace a las normas jurídicas dictadas en el ámbito de la actividad de tratamiento de datos personales.

Desde esta perspectiva, cobran especial relevancia los estándares internacionales que han buscado establecer una equivalencia normativa, siendo especialmente importante el estándar europeo actual, contenido en el Reglamento General de Protección de Datos de Europa y en el Convenio Nº 108, de 1981.

Nuestro país no es ajeno a esta realidad, habiendo regulado la materia en el año 1999 a través de la Ley Nº 19.628 sobre protección de la vida privada, hoy sometida a un proceso de revisión, tras verse superada por el avance tecnológico y los estándares internacionales actualizados. Por ello, si bien nos referiremos a ella cuando sea pertinente, también adelantaremos opinión sobre la manera en que debe ser reformada, teniendo a la vista los proyectos de ley en tramitación y los estándares internacionales vigentes.

Atendido el hecho de está dirigida primordialmente a miembros del escalafón primario del Poder Judicial, se ha intentado proponer ejemplos concretos de aplicación de las normas a casos reales, ocurridos tanto en Chile como en el derecho comparado. Si bien realizamos algunos juicios respecto de si la normativa fue correctamente aplicada o no, las referencias se hacen desde lo doctrinario y en la comprensión de que se trata de un asunto complejo, con ribetes técnicos no siempre susceptibles de ser aprehendidos por los hombres y mujeres de derecho, por lo que muchas veces se requerirá de la leal colaboración de los profesionales de las ciencias para una cabal comprensión de los hechos.



La problemática de la protección de datos personales

← Índice de contenidos

1.1 Antecedentes históricos del derecho fundamental a la protección de datos

Hasta inicios de la década de 1980, los países pertenecientes a los sistemas jurídicos de derecho continental europeo, como Chile, enfrentaban un problema singular: el desarrollo de las tecnologías de la información –en particular el procesamiento automatizado de los datos de las personas– cada vez se aplicaba más en la adopción de decisiones respecto de los individuos, muchas de las cuales vulneraban sus derechos fundamentales.

Esto se reflejaba, por ejemplo, en la injustificada denegación de créditos, la negativa a ofrecer seguros de salud, el cierre del acceso a determinados colegios, la imposibilidad de arrendar viviendas, la negativa a contratar como trabajador a personas evidentemente competentes, y un largo etcétera de sinsabores sin justificación aparente.

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

¿Cómo restablecer el imperio del derecho en este contexto? A eso se aboca el derecho a la protección de datos personales.

1.2 El precedente: la *Privacy* norteamericana

La idea de protección frente a las tecnologías ha recorrido un largo camino hasta llegar a adquirir las formas que hoy conocemos. En los albores de su desarrollo, se advirtió acerca de los riesgos que podía representar la prensa y sus "modernas tecnologías" (en su momento, la cámara fotográfica y la imprenta). En este contexto se acuñó la antigua institución de derecho norteamericano conocida como *Privacy*, cuyos orígenes se remontan a la sistematización que hicieran de ella Louis Dembitz Brandeis y Samuel Dennis Warren, quienes, a partir de precedentes jurisprudenciales, publicaron su artículo "*The Right of Privacy*"[1]. Concebido como "*the right to be let alone*", esto es, "el derecho a ser dejado solo", a no ser molestado, lo que lleva aparejado como consecuencia que se prohíba a terceros controlar la información que pertenece a una persona, a quien se le reconoce la propiedad de su información.

Esta tesis obedece a una construcción *ius privatista* de las garantías personales, que desarrolló su argumentación a partir del derecho de propiedad (*property*), específicamente de un atributo de los derechos de autor como es el derecho al inédito, esto es, a no publicar sus obras o, en este caso, las actuaciones de los individuos.[2]

1 Fue publicado originalmente en *Harvard Law Review*, vol. IV, Nº 5 (1890) y traducido al castellano por Benigno Pendás y Pilar Baselga como *El derecho a la intimidad*, siendo publicado por editorial Civitas en Madrid, en 1995. La traducción del título a nuestro idioma es errónea, lo que ha dado lugar a una de las transferencias de conocimiento más lamentables y perdurables del ámbito jurídico, pues en realidad debió llamarse "El derecho a la privacidad", ya que intimidad y *privacy* son instituciones jurídicas provenientes de sistemas jurídicos distintos y con características propias y diferenciadas.

2 Específicamente el artículo nace como una forma de reacción de Samuel D. Warren, adinerado empresario del papel y famoso personaje de la vida social y política norteamericana, cuyas fiestas y *affaires* eran el comidillo de los periódicos de la época en la ciudad de Boston, los cuales le perseguían, cámara fotográfica en ristre, para luego publicar en diarios y revistas noticias sobre él y su familia con detalles personales altamente desagradables. Warren acudió a su compañero de estudios en Harvard, Louis Dembitz Brandeis, quien llegaría a ser juez de la Corte Suprema, y publicaron en conjunto el artículo en referencia, uno de los más influyentes del ordenamiento jurídico norteamericano.

Desde entonces, el derecho a la privacidad es la fórmula que satisfizo al derecho norteamericano para enfrentar la capacidad invasiva de los periódicos y la prensa en general, así como las tecnologías de las que disponían, como un escudo o límite a su intromisión en la vida de las personas de finales del siglo XIX.

Por supuesto que esta idea no se corresponde con las dimensiones que ha adquirido en nuestros días, pues al no existir ninguna barrera jurídico-constitucional que defina o delimite lo que es *the right of privacy*, la garantía ha ido ampliando sucesivamente sus contornos por vía jurisprudencial, para adecuarse a las nuevas necesidades sociales, políticas y económicas, hasta incluir a la información de las personas tratadas a través de sistemas automatizados de información. Incluso existe consenso en que *Privacy* es un derecho constitucionalmente protegido, aun cuando la Constitución de Estados Unidos no la reconoce expresamente.[3]

Es así como hoy *Privacy* abarca un conjunto heterogéneo de contenidos: el domicilio, la facultad de guardar silencio sobre opiniones, actividad política y/o pertenencia a asociaciones, el derecho de la mujer a interrumpir su embarazo dentro de los tres meses posteriores a la concepción, el tener revistas y materiales pornográficos en casa, medidas sancionatorias hacia los estudiantes por contraer matrimonio, promiscuidad sexual, prohibición de obtener pruebas por medios ilícitos, convivencia extramatrimonial y un largo –larguísimo– etcétera que hace imposible llegar al núcleo de su contenido.[4]

Al no existir un concepto unitario de *Privacy*, no hay límite a los objetos que tutela: es un concepto jurídicamente indeterminado, por lo que en el sistema norteamericano la irrupción de la tecnología

3 Este tipo de prácticas no son del todo ajenas a los sistemas jurídicos basados en derecho continental, baste recordar por ejemplo que el derecho a vivir en un ambiente libre de contaminación, que arranca de la interpretación que los tribunales europeos hicieron de la Convención Europea de Derechos Humanos de 1950, y que recorrió con gran éxito el mundo entero, no estaba en la Convención. Es una creación jurisprudencial, lo que explica también lo apremiante que resultó la adopción de la Constitución Europea: existían derechos sin soporte legislativo, cuestión que la Carta solucionaba.

4 A quienes interese un análisis detallado de los supuestos que puede llegar a cubrir el concepto de *Privacy*, recomendamos el trabajo de Enzo Roppo "Il diritti della personalità" en *Banche dati, telematica e diritti della persona*, edición al cuidado de Mario Bessone, Cedam, Padua, 1984, pp. 64 y 65.

informática no provocó grandes debates, ya que como bien señala Serrano, "los contornos de la *privacy* no son definibles *a priori*, puesto que estos son perfilados de forma casuística y en lógica relación con los avances de la sociedad, por lo que, de igual manera, también resulta difícil dar una definición a posteriori de la misma".[5] Además nos revela, tal como explica González Hoch, que el sentido en que un abogado formado en la tradición del *common law* emplea la palabra *privacy* es muy distinto al sentido que atribuye al término "privacidad" un abogado formado en la tradición del derecho continental (incluyendo al chileno) y que "el empleo de términos en apariencia semejantes pero con significados distintos puede conducir a graves confusiones, tanto en el lenguaje corriente como en el lenguaje especializado del Derecho".[6]

Sin perjuicio de lo recién señalado, debe admitirse que el concepto de *privacy* o privacidad goza de gran popularidad a nivel mundial, y también en nuestro país, aun cuando es propio del sistema jurídico norteamericano y en Chile –en sentido estrictamente dogmático-jurídico– carece de contenido.[7]

Su popularidad se explica en razón de que, con el desarrollo de internet y la generación de sitios web, estos últimos comenzaron a publicar declaraciones de exención de responsabilidad bajo el título de *privacy policy*, las que se copiaron y tradujeron mundialmente como "políticas de privacidad", generándose una confusión conceptual con la que convivimos en el día a día, sobre todo considerando que los tratados internacionales consagran como derecho la "vida privada", concepto similar pero jurídicamente diferente a la *privacy* norteamericana.

5 María Mercedes Serrano Pérez, *El derecho fundamental a la protección de datos. Derecho español y comparado*, Civitas, Madrid, 2003; p. 32.

6 Francisco González Hoch, "Modelos comparados de protección de la información digital y la ley chilena de datos de carácter personal". En *Tratamiento de datos personales y protección de la vida privada*, edición al cuidado de Jorge Wahl Silva, Ediciones Universidad de los Andes, Santiago de Chile, 2001; p. 153.

7 Quizás uno de los esfuerzos más exóticos por dotar de contenido al concepto de *privacidad* es el de Figueroa García-Huidobro, que en su obra homónima toma la doctrina y jurisprudencia norteamericana sobre indemnización de perjuicios para analizar su contenido y deducir que, en Chile, la privacidad es un derecho fundamental que ampara determinados cuerpos, objetos y espacios, a pesar de que tal concepto no está ni en la Constitución ni en las leyes. Rodolfo Figueroa García-Huidobro, *Privacidad*, Ediciones Universidad Diego Portales, Santiago de Chile, 2014.

El derecho a ser dejado solo por los medios de comunicación social marca el inicio del desarrollo de la *Privacy* norteamericana. Esta noción reconoce la propiedad de la persona respecto de la información que le concierne, además de muchas otras extensiones, tales como el derecho al inédito de la obra propia, el derecho a no ser denostado, entre otros.

El derecho a ser dejado solo por los medios de comunicación social marca el inicio del desarrollo de la *Privacy* norteamericana. Esta noción reconoce la propiedad de la persona respecto de la información que le concierne, además de muchas otras extensiones, tales como el derecho al inédito de la obra propia, el derecho a no ser denostado, entre otros.

1.3 La vía europea principal: la intimidad

A diferencia del sistema norteamericano, que creó la *privacy* en el siglo XIX como una institución jurídica flexible, que fue modelándose conforme se presentaban casos de afectación a los derechos de las personas, el derecho continental europeo no poseía ninguna figura semejante al *right of privacy*, por lo que inició una larga peregrinación en busca de la construcción jurídica de una garantía para la protección de los derechos de las personas.

En este entorno, inició ese recorrido desde la intimidad, el derecho al honor y a la propia imagen, enfoque que fue cobrando progresiva relevancia atendido el avance del desarrollo tecnológico y su capacidad invasiva, para luego replantearse el rol de la idea de "vida privada" contemplada en tratados internacionales, aunque siempre manteniendo en el centro la dignidad de la persona y su autodeterminación.

De hecho, es esta corriente la que da lugar a las primeras manifestaciones normativas de la protección de datos personales, a través del Convenio Nº 108 del Consejo de Europa, de 28 de enero de 1981, para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, donde se reconoce expresamente "que es deseable ampliar la protección de los derechos y de las libertades fundamentales de cada uno, concretamente el derecho al respeto de la vida privada, teniendo en cuenta la intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamientos automatizados".

Sin embargo, ¿por qué recurrir ahora a esa vaga "vida privada" de los tratados internacionales como esfera de protección, cuando la mayoría de las legislaciones nacionales de derecho continental siempre había considerado suficiente la protección que brindaba el derecho a la "intimidad" de los individuos?

Porque la intimidad se sitúa en "el ámbito de los pensamientos de cada cual, de la formación de sus decisiones, de las dudas que escapan a una clara formulación, de lo reprimido, de lo aún no expresado

que quizá nunca lo será, no solo porque no se desea expresarlo sino porque es inexpresable"[8], y por ende, escasa relación puede tener con los datos e informaciones que circulen respecto de las personas y su vinculación en el lenguaje popular ha traído más confusiones que protección a los derechos de las personas.

Por ejemplo, los datos de afiliación sindical, ¿son datos íntimos? No, de hecho son datos que permiten o traducen el esfuerzo colectivo y público de grupos de personas organizadas para conseguir determinados fines en el entorno laboral. ¿Son entonces datos de la vida privada? Tampoco parecen serlo, y tal vez ello sea una de las razones que explican el posterior abandono de la noción o idea de que la vida privada era una institución suficiente como para proteger a las personas contra los abusos de, por ejemplo, la libertad de información u opinión. Es por ello que existe un conjunto de informaciones relativas a personas, lesivas para sus derechos, que no tienen relación alguna con la intimidad o con la vida privada, pero cuya circulación indiscriminada puede acarrear desastrosas consecuencias como, por ejemplo, negarle a una persona el acceso al mercado del trabajo por el hecho de haber ejercido su legítimo derecho a sindicalizarse. Por tanto, si bien son datos públicos, se los incluye dentro de los datos sensibles.

Frente a esta disyuntiva, el Tribunal Constitucional de España aclaró expresamente que el derecho fundamental a la intimidad no aporta por sí solo una protección suficiente frente a las realidades nuevas derivadas del progreso tecnológico, por lo que la Constitución, al establecer que la ley debe limitar el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos, pone de manifiesto la existencia de los riesgos asociados a ese progreso, encomendando al legislador el desarrollo de garantías, que también son, en sí mismas, un derecho o libertad fundamental.[9]

8 Ernesto Garzón Valdés, "Lo íntimo, lo público y lo privado". En *Cuadernos de Transparencia* 06, Instituto Federal de Acceso a la Información Pública, Ciudad de México, 2015; p. 15.

9 Sentencia del Tribunal Constitucional de España 254/1993, de 20 de julio de 1993 (ECLI:ES:TC:1993:254), reiterada en sentencia 58/2018, de 4 de junio de 2018 (ECLI:ES:TC:2018:58).

1.4 El aporte alemán: derecho a la autodeterminación informativa

Al igual que el resto de los países de Europa, en el ordenamiento jurídico de Alemania no existe la *Privacy* ni se la ha recogido; tampoco existe la "intimidad" en su Ley Fundamental (*Grundgesetz*), pero sí ampara la dignidad de la persona (1.1) y el libre desarrollo de la personalidad (2.1).[10] Esto les permitió construir el derecho a la autodeterminación informativa a través de una sentencia del Tribunal Constitucional de la República Federal de Alemania[11], que declaró como violatorio de la *Grundgesetz* algunos preceptos de la Ley de Censo de 1982.[12] Dicha sentencia reconoció que:

> "En las condiciones de la elaboración moderna de datos, la protección del individuo contra la recogida, almacenamiento, utilización y difusión ilimitada de sus datos personales queda englobada en el derecho general de protección de la persona del artículo 2º, párrafo 1 [*derecho general a la propia personalidad*], en relación con el artículo 1º del párrafo 1 [*protección de la dignidad humana*] de la ley fundamental. El derecho constitucional garantiza en esta medida la facultad del individuo de determinar fundamentalmente por sí mismo la divulgación y utilización de los datos referentes a su persona".

Siendo así, se independiza la protección de datos personales respecto de la intimidad, el honor y la propia imagen como garantías protegidas y recalca la función instrumental a la protección de la dignidad,

10 Todos tienen derecho al libre desarrollo de su personalidad en tanto en cuanto no lesione los derechos ajenos y no contravenga el orden constitucional o las buenas costumbres".

11 Todos los fragmentos de la sentencia que en adelante reproduciremos corresponden a la traducción que hizo de la misma Manuel Daranas, publicada en el *Boletín de Jurisprudencia Constitucional* N° 33 de las Cortes Generales, Madrid, 1984; pp. 126-170 (lo encerrado entre corchetes es de los autores).

12 Esta ley, aprobada por unanimidad y sin mayor debate por el *Bundestag*, compelía a responder a las más de 100 preguntas del Censo poblacional correspondiente. Dada la entidad y cantidad de las interrogantes, algunos ciudadanos se negaron a responderlas, por lo que el Estado accionó contra ellos con las consecuencias que se traducen en la referida sentencia.

la libertad y la igualdad que asisten a la persona humana en general, de las que derivan la generalidad de las garantías consagradas en los distintos catálogos de derechos.

Conforme a ello, realiza una construcción a través de la cual reconoce la existencia del derecho a la autodeterminación informativa, que emana directamente de la dignidad de la persona, la cual, en tanto sujeto de derecho, actúa con autodeterminación como miembro de una sociedad libre.

También considera los peligros que entrañan para estos bienes jurídicos las condiciones imperantes en esa época y las que visualiza a futuro respecto de la elaboración automática de datos. Conforme a ello, sostiene que la necesidad de garantizar la autodeterminación demanda un nivel especial de protección, por cuanto este derecho faculta al individuo para decidir por sí mismo cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida, de lo que se deduce "la libre eclosión de la personalidad del individuo contra la recogida, el almacenamiento, la utilización y la transmisión ilimitada de los datos concernientes a la persona".

Como cualquier otro, el Tribunal Constitucional alemán reconoce que este derecho no es absoluto; sin embargo, las limitaciones que a su respecto se impongan:

> "Solo son admisibles en el marco de un interés general y necesitan un fundamento legal basado en la Constitución, que debe corresponder al imperativo de claridad normativa, inherente al Estado de Derecho. En su regulación debe el legislador observar, además, el principio de la proporcionalidad y tiene que adoptar asimismo precauciones de índole organizativa y de derecho a la salvaguardia de la personalidad".

Tan evidente es la vinculación de este derecho a la libertad y autodeterminación del individuo, que la sentencia entiende que la conducta de la persona podrá verse afectada severamente a través de su vulneración. Así, sostiene que:

> "El que [*la persona*] no pueda percibir con seguridad suficiente qué informaciones relativas a él son conocidas en determinados sectores de su entorno social, y quien de alguna manera no sea capaz de aquilatar lo que puedan saber de él sus posibles comunicantes, puede verse sustancialmente cohibido en su libertad de planificar o decidir por autodeterminación (…) Quien se siente inseguro de si en todo momento se registran cualesquiera comportamientos divergentes y se catalogan, utilizan o transmiten permanentemente a título de información procurará no llamar la atención con esa clase de comportamiento. Quien sepa de antemano que su participación, por ejemplo, en una reunión o iniciativa cívica va a ser registrada por las autoridades y que podrán derivarse riesgos para él por este motivo renunciará presumiblemente a lo que supone un ejercicio de los correspondientes derechos fundamentales (…) esto no solo menoscabaría las oportunidades de desarrollo de la personalidad individual, sino también el bien público, porque la autodeterminación constituye una condición elemental de funcionamiento de toda comunidad fundada en la capacidad de obrar y de cooperación de los ciudadanos".

La autodeterminación informativa es el derecho del individuo a controlar la obtención, tenencia, tratamiento y transmisión de datos relativos a su persona, decidiendo en cuanto a los mismos las condiciones en que dichas operaciones pueden llevarse a cabo.

Es decir, la autodeterminación informativa se construye bajo un fundamento constitucional distinto de la intimidad.[13] ¿Cómo podemos definirla entonces?

La autodeterminación informativa es el derecho del individuo a controlar la obtención, tenencia, tratamiento y transmisión de datos relativos a su persona, decidiendo en cuanto a los mismos las condiciones en que dichas operaciones pueden llevarse a cabo. Se trata de controlar la utilización de las informaciones personales indepen-

13 Debe tenerse presente que el derecho a la protección de los datos personales como tal (no nos estamos refiriendo a la *Privacy*) se entiende de manera distinta en el sistema del *common law* y particularmente en el ordenamiento jurídico norteamericano. "La principal diferencia entre Europa y EE. UU. es que el derecho a la protección de datos en el viejo continente es percibido como derecho fundamental mientras que en EE. UU. es vista como una problemática del derecho de la defensa de la competencia y defensa de los derechos de los consumidores", señala María Álvarez Caro en *Derecho al olvido en internet: el nuevo paradigma de la privacidad en la era digital*, Reus, Madrid, 2015; p. 87. Su observación es coincidente con las visitas al país, durante la primera presidencia de Sebastián Piñera (2010-2014), de miembros del Departamento de Comercio de EE. UU., quienes venían a explicar al Servicio Nacional del Consumidor (Sernac) lo que ellos entendían por derecho a la protección de datos personales desde su particular óptica, lo que redundó en un intento legislativo (Boletín N° 8143-03) de constituir al Sernac en una de las autoridades de protección de datos del país.

dientemente si éstas pueden ser calificadas de íntimas, reservadas, secretas, privadas: no es relevante su mayor o menor proximidad con el ámbito o núcleo íntimo de las personas.

En el caso español, si bien se comparte el razonamiento del Tribunal Constitucional alemán, se opta por el término "libertad informática".

En síntesis, respecto de la figura jurídica que protege a las personas frente al tratamiento abusivo de sus datos, encontramos dos realidades:

<table>
<tr><th>Common law norteamericano</th><th colspan="2">Derecho continental europeo</th></tr>
<tr><td rowspan="2">Derecho a la privacidad ("Privacy")</td><td colspan="2">Derecho a la protección de datos personales</td></tr>
<tr><td>TC alemán: autodeterminación informativa</td><td>TC español: libertad informática</td></tr>
</table>

1.5 La autodeterminación informativa y su recogida en Chile

A partir del pronunciamiento del Constitucional alemán, surge una abundante normativa que acompaña el proceso de consolidación de este derecho y que va reflejando los giros legislativos y las experiencias de los países.

Dentro de este contexto, a nivel internacional son referentes obligados las Directrices para la Regulación de los Archivos Personales Informatizados, adoptadas por la Organización de las Naciones Unidas (ONU) mediante Resolución 45/95 de la Asamblea General, de 14 de diciembre de 1990, y a nivel europeo, el Convenio Nº 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal[14], como también la hoy derogada Directiva Europea 95/46/CE, que sentó los principios base en materia de protección de datos personales para el entorno comunitario y en cuyo rol ha sido sustituida desde el año 2018 por el actual Reglamento General de Protección de Datos (RGPD).[15]

En Chile, nuestro Tribunal Constitucional (TCCh), en junio del año 2011 también tuvo ocasión de referirse a la autodeterminación informativa y lo hizo señalando que "la protección de la vida privada de las personas guarda una estrecha relación con la protección de los datos personales, configurando lo que la doctrina llama derecho a la autodeterminación informativa"[16], y que la Ley Nº 19.628, sobre protección de la vida privada, era consecuente con ello.

14 El Convenio N° 108 fue el primer instrumento internacional jurídicamente vinculante adoptado en el ámbito de la protección de datos, y todavía se encuentra vigente. Tiene como fin garantizar a cualquier persona física "el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona".

15 Formalmente su nombre es "Reglamento (UE) 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 y por el que se deroga la Directiva 95/46/CE", que entró en vigencia el 25 de mayo de 2018.

16 Sentencia del Tribunal Constitucional de Chile, de 21 de junio de 2011, recaída en la causa rol Nº 1.800-2010.

Más tarde, al mes siguiente, este mismo tribunal dijo derechamente que entendía que dicha ley "resguarda lo que se denomina derecho de la autodeterminación informativa. Es decir, se encarga de proteger a las personas de la circulación de la información que sobre ellas mismas existe en distintos centros de acopio". De esta manera, se reconoció la dimensión activa del derecho a la vida privada y no solo la faceta pasiva, entendida como la no interferencia ilegítima en la vida personal, el derecho a no ser molestado o a ser dejado solo. El derecho a la autodeterminación, en cambio, implica "controlar los datos que circulan sobre cada uno de nosotros".[17]

Es así como entre 1999 y 2018, el derecho a la autodeterminación informativa fue recogido por nuestra legislación como parte del derecho constitucional a la vida privada. En estas circunstancias, la Ley Nº 19.628 de 1999[18] fue titulada "Sobre protección de la vida privada" y proclama su labor de integración desde los primeros párrafos de la moción parlamentaria que inició su tramitación legislativa: "Sometemos a consideración del Senado un proyecto de ley que viene a llenar un vacío manifiesto en nuestro ordenamiento jurídico y cuyo propósito es dar una adecuada protección al derecho a la privacidad de las personas, en el ámbito del Derecho Civil, ante a eventuales intromisiones ilegítimas". Además, la moción señala el fundamento constitucional del que dice arrancar: "Partiendo del precepto contenido en el artículo 19 Nº4 de nuestra Carta Fundamental, nuestra moción comienza anunciando la inviolabilidad de la vida privada y advirtiendo que toda intromisión en la misma es, en principio, ilegítima".

Sin embargo, el legislador no advirtió que el artículo 19 Nº 4 en realidad contenía tres garantías diferentes: i) la protección de la vida privada, ii) la protección de la vida pública y iii) la protección de la honra de las personas. Si bien más adelante se modificó este artículo eliminando la protección a la vida pública, la honra siguió manteniendo una protección relativa a la información de las personas en dicho ámbito.

17 Sentencia del Tribunal Constitucional de Chile, de 12 de julio de 2011, recaída en la causa rol Nº 1.894-2011.
18 Moción del senador Eugenio Cantuarias Larrondo, de 5 de enero de 1993.

Demás esta señalar que el texto constitucional vigente a esa época no consideraba la protección de las personas frente al tratamiento automatizado de sus datos personales, porque no se advertían los ribetes que alcanzaría el desarrollo tecnológico en este ámbito.

Adicionalmente, si bien la Ley Nº 19.628 fue titulada "Sobre protección de la vida privada" y se la ancló en el artículo 19 Nº 4, no regula el derecho a la vida privada, puesto que los datos personales no tienen una relación necesaria con la esfera privada de las personas. Lo que hace la ley es establecer reglas relativas al mercado de los datos personales, esto es, principalmente, al tratamiento de datos de carácter económico, cuyo principal gestor en aquel entonces era la empresa Dicom.[19] De hecho, parte importante de la jurisprudencia relativa a esta ley, de esa época, se refiere a casos relativos al tratamiento de datos realizado por esa empresa.

Afortunadamente, hoy ya no es necesario mantener el *anclaje* de la protección de datos en la protección de la vida privada, porque el 16 de junio de 2018 entró en vigor la Ley Nº 21.096, que modifica la Constitución Política de la República y consagra expresamente el derecho a la protección de datos personales bajo la fórmula siguiente:

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

Como consecuencia de esto, en la sesión del Senado que estudia las reformas a la actual Ley Nº19.628, los legisladores acordaron cambiarle el nombre a la ley "Sobre protección de la vida privada" y, de aprobarse el texto legislativo, se denominará derechamente "Sobre

19 Dicom, después Dicom-Equifax o solo Equifax, es una empresa gestora de información relativa al comportamiento financiero y comercial de las persona y empresas que, durante muchos años, mantuvo el cuasi-monopolio de las consultas para la evaluación del riesgo crediticio, llegando a extremos de ser decisiva para obtener un trabajo e incluso para arrendar vivienda: prácticamente ninguna decisión relativa a personas se tomaba sin consultar a Dicom y solo sucesivas reformas legislativas morigeraron su posición.

protección de datos personales"[20], para adecuar la norma a la nueva realidad jurídica y ajustarla a la correcta formulación de las garantías constitucionales consagradas en el artículo 19 Nº 4 CPR.

Garantías consagradas en el artículo 19 Nº 4 de la Constitución Política		
Protección de la vida privada	Resguardo de las esferas de la vida de la persona que desea mantener fuera del conocimiento de terceros.	Las tres garantías tienen en común que se refieren a la protección de la persona frente al uso que terceros hacen de la información de las personas.
Protección de la honra	Resguardo del buen nombre, buena fama o prestigio de la persona.	
Protección de datos personales	Derecho a controlar el uso que hacen terceros respecto de los datos personales que nos conciernen.	

Entonces, si la protección de datos es ahora un derecho fundamental[21], ¿cuál es su contenido, quiénes son los titulares y quiénes son los obligados?

Respecto del contenido, y en palabras de Gómez Sánchez, "consiste en un poder de disposición y de control sobre los datos personales quefaculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esosdatos personales para que, pudiendo oponerse a esa posesión o uso".[22]

Los titulares de este derecho son las personas naturales, sean nacionales o extranjeras, y los sujetos obligados, o sujeto pasivo, son tanto las personas naturales como las personas jurídicas privadas y el Estado.

20 Tal decisión está contenida en el Segundo Informe de la Comisión de Constitución, Legislación, Justicia y Reglamento recaído en el proyecto de ley, en primer trámite constitucional, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales, que se tramita a partir de los boletines Nº 11.092-07 y Nº 11.144 -07, refundidos.

21 Coincidentemente, también el Reglamento General de Protección de Datos, que había entrado en vigencia el mes anterior, declara que el derecho a la protección de datos personales es un derecho fundamental, aunque sus fundamentos son la Carta de Derechos Fundamentales de la Unión Europea y el Tratado de Funcionamiento de la Unión Europea.

22 GÓMEZ SÁNCHEZ, Yolanda, *Derechos fundamentales*, Aranzadi, Cizur Menor, 2018; p. 286.

En el caso del Estado, además de dar pleno cumplimiento a las normas y principios de protección de datos, debe adoptar todas las medidas que sean necesarias para asegurar la efectiva vigencia del derecho que se reconoce a las personas, lo que incluye adoptar medidas legislativas, reglamentarias y de organización, que permitan a las personas el ejercicio de sus facultades de disposición y control sobre sus propios datos.

Así, por ejemplo, y de acuerdo a los estándares internacionales, para la efectiva implementación de este derecho constitucional no basta dictar leyes que contengan lo principios y derechos generalmente aceptados, sino también habrá que establecer una autoridad independiente que vele por el efectivo respecto de este derecho, además de establecer sanciones que constituyan un real desincentivo a la vulneración del mismo.

1.6 Conceptos esenciales: datos, banco de datos, tratamiento y responsables

En materia de protección de datos personales, existen cuatro pilares fundamentales que hay que retener, no solo porque son las bases del derecho a la protección de datos personales, sino también porque internacionalmente son bastante uniformes. Se trata de los conceptos de **datos personales**, **tratamiento de datos**, **registro o banco de datos** y **sujetos del tratamiento**.

Respecto de los sujetos del tratamiento, tenemos a los responsables del tratamiento de datos, concepto que distingue entre el responsable del registro o banco de datos propiamente tal, esto es, la persona natural o jurídica que decide sobre la recopilación, uso y destino de los datos, y el prestador de servicios de tratamiento, que es la persona natural o jurídica, distinta de la persona responsable, que lleva a cabo el tratamiento de datos de carácter personal por encargo de dicha persona responsable.

La legislación internacional también releva la existencia de la persona del **interesado**, denominación que se refiere a la persona natural cuyos datos de carácter personal son objeto de tratamiento.

Responsable del banco de datos	Responsable del tratamiento	Interesado
Persona natural o jurídica que decide sobre la recopilación, uso y destino de los datos.	Persona natural o jurídica que realiza operaciones de tratamiento de datos de carácter personal por encargo de la persona del responsable.	Persona natural a quien los datos se refieren, por lo que es el titular del derecho a la protección de datos.
Ejemplo: Universidad de Chile, a través de su representante legal.	Ejemplo: Juan Pérez, ingeniero de sistemas en la Universidad de Chile y/o la empresa tecnológica Sondéame SpA, por contrato con la Universidad de Chile.	Ejemplo: Santiago Sepúlveda, estudiante de Periodismo en la Universidad de Chile.

Nuestra Ley Nº 19.628 contiene las definiciones de los conceptos enunciados anteriormente, pero lo fundamental es tener presente que, de acuerdo a su artículo 1º, "el tratamiento de datos de carácter

personal en registros o bancos de datos por organismos públicos o por particulares se sujetará a las disposiciones de esta ley", lo que desde ya nos advierte que, en principio, la regulación no está dirigida solo hacia los particulares sino también hacia los organismos del Estado, y en segundo lugar, que se trata de una **ley de carácter general y supletorio**.

Luego, en su artículo 2º, nos indica lo que entiende por **datos personales**, siendo estos "los relativos a cualquier información concerniente a personas naturales, identificadas o identificables", debiendo destacarse entre los elementos que forman el concepto, que comprende "cualquier información", por tanto, el concepto es amplio en varios sentidos.

En primer lugar, los datos personales comprenden **todo tipo de datos que se refieran a una persona** y lo serán **con independencia de su naturaleza y forma de representación**, ya sea imagen, sonido, o conjunto de caracteres grafológicos, muestras biológicas, etcétera.

En segundo lugar, estos datos se refieren a una **persona física o natural**. Por tanto, no es dato personal aquel que aporta información en relación a una persona jurídica. Esta es la tendencia generalmente adoptada por los Estados que entienden que la protección deriva directamente de la dignidad humana.

Finalmente, el concepto restringe la protección a los datos que sean atribuibles a personas identificadas o identificables. Al respecto, las dudas suelen producirse respecto de la expresión "identificable", en el sentido de determinar cuándo considerar que los esfuerzos para llegar a una identificación concreta (a partir de un dato) son tan desmedidos, que prácticamente no lo podemos asociar a una persona, como podría ser intentar identificar a alguien entre millones de personas a partir de un dato aislado, por ejemplo "el sujeto de pelo castaño".

En un primer momento, las reflexiones sobre este punto fueron restrictivas; de hecho, el Convenio Nº 108 de la Unión Europea dispone que la persona es identificable si "puede ser fácilmente identificada; no se incluye al respecto la identificación de personas por métodos comple-

jos", con lo cual se excluía, de suyo, todo método de carácter científico o técnico de identificación, tales como el análisis de huellas dactilares, el procesamiento de imágenes o sonidos, o el análisis de ADN.

Pero actualmente, el criterio aplicado a nivel internacional es el del Reglamento General de Protección de Datos de Europa (RGPD), que como señalamos entró en vigor el año 2018 y en cuyo artículo 4 número 1 define dato personal como "toda información sobre una persona física identificada o identificable ('el interesado'); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona", con lo cual se reconoce el amplio espectro de posibilidades para llegar a la identidad de la persona.

También debemos tener muy presente el concepto de **tratamiento de datos** u operaciones de tratamiento de datos personales, que está referido a cualquier operación o conjunto de operaciones, sean o no automatizadas, que se aplique a datos de carácter personal, en especial su recogida, conservación, utilización, revelación o supresión.

Al respecto, el artículo 2º de la Ley Nº 19.628 es un poco más descriptivo todavía, al entender que tratamiento de datos es "cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizados o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal o utilizarlos de cualquier forma".

Como podemos apreciar, la ley no se limita a los tratamientos automatizados de datos personales, sino que además regula los tratamientos manuales de información, como podría ser un sistema de registros llevados por escrito y, todavía más, la enumeración de verbos que contiene esta definición es meramente enunciativa, por lo que las

operaciones que pueden entenderse como tratamiento de datos está abierta a otras actividades, como puede ser la publicación de datos personales en páginas o sitios web.

En realidad, la forma de la descripción de actividades que hace nuestra ley, no es muy distinta al Reglamento europeo a que nos hemos referido, que define **tratamiento** en su artículo 4 número 2 como "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción".

Artículo 2º de la Ley Nº 19.628	Artículo 4 número 2 del RGPD
"cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizados o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal o utilizarlos de cualquier forma".	"cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción".

Respecto de lo que debemos de entender por **registro o banco de datos**, la Ley Nº 19.628 en su artículo 2º letra m nos dice que es "el conjunto organizado de datos de carácter personal, sea automatizado o no y cualquiera sea la forma o modalidad de su creación u organización, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos".

Internacionalmente, más que registro o banco de datos, se suele usar la expresión *fichero*, el cual, en su momento fue definido por la Directiva Europea 95/46/CE, como "todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido en forma funcional o

Cualquiera que sea el lado del Atlántico en que nos encontremos, el registro, banco de datos o *fichero* hace referencia a un conjunto estructurado de datos dotado de un sistema lógico de recuperación.

geográfica", concepto que fue asimismo recogido de forma idéntica en el Reglamento General de Protección de Datos de Europa, en su artículo 4, número 6.

Como podemos apreciar, cualquiera que sea el lado del Atlántico en que nos encontremos, el registro, banco de datos o *fichero* hace referencia a un conjunto estructurado de datos dotado de un sistema lógico de recuperación.

Ahora bien, el requisito de *estructuración* cobra relevancia tratándose de bancos de datos manuales, según hace notar el Reglamento europeo en su motivación número 15, en el cual señala: "A fin de evitar que haya un grave riesgo de elusión, la protección de las personas físicas debe ser tecnológicamente neutra y no debe depender de las técnicas utilizadas. La protección de las personas físicas debe aplicarse al tratamiento automatizado de datos personales, así como a su tratamiento manual, cuando los datos personales figuren en un fichero o estén destinados a ser incluidos en él. Los ficheros o conjuntos de ficheros, así como sus portadas, que no estén estructurados con arreglo a criterios específicos, no deben entrar en el ámbito de aplicación del presente Reglamento".

En el fondo, si determinada información personal consta en soportes físicos, como hojas de papel, sin que estén sistematizadas o estructuradas de forma alguna y, por ende, no es posible hacer recuperación de los datos en ellos contenidos pues es prácticamente imposible encontrarlos, en ese caso no sería aplicable la legislación de protección de datos, sin embargo la información contenida en sistemas informáticos, aun cuando no esté estructurada, se regirá por esta legislación y quedará amparada por la garantía fundamental.

1.7 Categorías de datos personales y sus implicancias desde la óptica de su protección

Existe consenso doctrinario en que no hay datos personales irrelevantes desde la óptica del resguardo del derecho que nos ocupa, pues hasta el más nimio de ellos posibilita, en combinación con otros, construir un acabado perfil de una persona y, así, quedar en posición de manipular incluso su voluntad y su entorno.

Quien conoce de esta forma a la persona podría modelar los estímulos a que la somete para obtener determinadas reacciones que son deseadas, un asunto de interés para mercados tan amplios como el de los productos y servicios, pero también para el de las convicciones y decisiones políticas a las que debe concurrir con su voluntad la persona.

La relevancia de cada dato personal estará dada por la posibilidad de que su tratamiento por terceros pueda acarrear discriminaciones arbitrarias en relación a la persona. Si el tratamiento de un tipo de dato acarrea un mayor riesgo de discriminación se le aplicará el régimen jurídico diferenciado de los "datos sensibles" o "datos especialmente protegidos".

La relevancia de cada dato personal estará dada por la posibilidad de que su tratamiento por terceros pueda acarrear discriminaciones arbitrarias en relación a la persona. Si el tratamiento de un tipo de dato acarrea un mayor riesgo de discriminación se le aplicará el régimen jurídico diferenciado de los "datos sensibles" o "datos especialmente protegidos".

Veamos cómo se refleja esto en nuestra Ley Nº 19.628: la ley reconoce que existen al menos dos categorías de datos personales diferentes: por una parte los datos personales que podríamos apellidar *a secas* y por otra están los datos personales *sensibles,* que el legislador denomina "datos sensibles", mientras que el regulador europeo los llama datos "especialmente protegidos".

Los datos personales, que para el solo efecto de esta explicación apellidaremos "a secas", son todos aquellos datos que no tienen restricciones excepcionales a su tratamiento, o por oposición, todos aquellos que no tienen el carácter de datos sensibles.

En cambio, los datos sensibles o especialmente protegidos son "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, 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".

Al respecto, la Resolución de Madrid se refiere a los datos sensibles como aquellos datos de carácter personal que puedan revelar aspectos como el origen racial o étnico, las opiniones políticas o las convicciones religiosas o filosóficas, así como los datos relativos a la salud o a la sexualidad: no se trata de un *numerus clausus*, sino que está abierto a cualquier otro tipo de datos que tengan esa capacidad o aptitud para el daño a sus titulares.[23]

Para el legislador, esta especial categoría de datos implica que puede y debe establecer garantías adicionales para preservar los derechos de los interesados.

¿Qué tienen de característico este tipo de datos? Si nos fijamos en la enumeración (que es meramente enunciativa), apreciaremos que algunos de ellos nada tienen que ver con la vida privada o con la intimidad, sino que se caracterizan porque su utilización indebida puede dar origen a una discriminación ilegal o arbitraria, o conllevar graves riesgos para la vida o seguridad de la persona.

En nuestra ley vigente, la enumeración de los datos sensibles no es taxativa, sino una lista abierta ("tales como…"), por lo que el encuadre de los datos personales en alguna de estas categorías dependerá de la apreciación que realicen los tribunales en cada caso concreto. Los tribunales perfectamente podrían determinar, por ejemplo, que la publicación que hacen las municipalidades de listados, con nombres y apellidos, de personas beneficiarias de programas sociales, es incompatible con la Ley Nº 19.628, pues se trata de datos sensibles que exponen a las personas a la vergüenza, al escarnio o al aprovechamiento por terceros de su situación de vulnerabilidad.

23 Artículo 2° de la Ley N°19.628, de 1999: "Para los efectos de esta ley se entenderá por (…) g) Datos sensibles, 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, 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".

Respecto de los datos sensibles, el artículo 10 de la Ley Nº 19.628 es enfático: "No pueden ser objeto de tratamiento los datos sensibles, salvo cuando la ley lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares".

Además, a nivel doctrinario se reconoce que quienes se dedican a tratar datos sensibles, ya sea por autorización legislativa o por consentimiento del propio titular de los datos, están obligados a tomar todos los resguardos jurídicos, organizativos y técnicos para que ellos solo puedan ser conocidos y utilizados en el ámbito en que su uso sea necesario y aceptable, pero manteniendo siempre medidas de seguridad incluso superiores a otros tipos de datos personales. En el fondo, estamos hablando de que al responsable del tratamiento de datos sensibles le es exigible una máxima diligencia.

Ahora bien, nuestra Ley Nº 19.628 dedica una extensa regulación a una categoría especial de datos, aunque no se menciona como tal, pero que ocupa un rol nuclear en ella: nos referimos a los datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial, que se regularon especialmente en el Título III, titulado "De la utilización de datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial", que establece el régimen aplicable tanto a datos relevantes para los procesos de marketing como a aquellos necesarios para la determinación de la solvencia patrimonial y riesgo financiero de las personas. A este respecto, a través de la Ley Nº 20.575, interpretativa de la Ley Nº 19.628, se regula detalladamente la finalidad del tratamiento, la elaboración de evaluadores de riesgo comercial, el consentimiento del interesado, el plazo de tratamiento de datos e, incluso, cómo se concretan los principios del tratamiento de datos personales en esta materia.

Tipos de datos personales	
Datos personales sensibles o especialmente protegidos	Aquellos cuyo tratamiento por parte de terceros puede redundar en discriminaciones arbitrarias respecto de la persona, por lo que el legislador prevé hipótesis estrictas de legitimación.
Datos personales (a secas)	Aquellos que se refieren a información de las personas que es necesaria para la gestión de las relaciones sociales, comerciales o civiles de la persona por lo que la ley, como regla general faculta a terceros a tratarla.
Datos de carácter económico, financiero, bancario o comercial	Sin ser una categoría distinta de los datos personales ordinarios, su contenido es detalladamente regulado por el legislador por su impacto en el mercado.

Tal es la relevancia de los datos económicos, que parte importante de la jurisprudencia se refiere a conflictos en relación al tratamiento de este tipo de información. A continuación se reseñan algunos de ellos, haciendo presente que, atendida la reforma constitucional, hemos privilegiado la jurisprudencia desde 2020 a la fecha, para lo cual hemos considerado como fuente la base de datos de jurisprudencia del Poder Judicial.

Rol/fecha/procedimiento	Doctrina
Nº 112.543-2020, 17 de febrero de 2021. **Recurso de protección (parcialmente acogido)**	Transgrede lo previsto en el artículo 17 inciso segundo de la Ley Nº 19.628, la publicación de la información sobre una deuda correspondiente a línea de crédito para estudiantes de educación superior con garantía estatal según Ley Nº 20.027 con el Banco del Desarrollo. "El informe de deudas, o Estado de Deudores, como lo llama la Comisión para el Mercado Financiero, por tratarse del almacenamiento, registro o conservación de información en un banco de datos a que se refieren los artículos 1 y 2 de la Ley N° 19.628, se encuentra sujeto al límite de respetar el pleno ejercicio de los derechos fundamentales de los titulares de los datos, cuestión que implica que no solo las entidades bancarias, sino que también la autoridad, ha de respetar el claro tenor del inciso segundo del artículo 17 antes referido" (CS, considerando 7º). "La comunicación por la Comisión para el Mercado Financiero de la deuda en comento constituye un acto ilegal y arbitrario, en cuanto no solo vulnera la expresa prohibición contenida en el inciso 2° del artículo 17 de la Ley N° 19.628, sino que, además, carece de todo fundamento que la justifique, pues el legislador ha sido claro al prohibir la comunicación, en cualquier caso y supuesto, de deudas como aquella que es materia de autos, con lo que el citado ente estatal vulnera, a su vez, el derecho establecido en el N° 4 del artículo 19 de la Constitución Política de la República, al afectar la honra de la persona a quien se refieren los datos de carácter personal informados" (CS, considerando 8º).

Nº 24469-2020, 10 de noviembre de 2020. **Recurso de protección (acogido)**	"El registro de deuda castigada al que hace referencia la institución financiera recurrida, se encuentra regido por la Ley N° 19.628, por tratarse del almacenamiento, registro o banco de datos a los que se refieren sus artículos 1 y 2 y, por consiguiente, sujeto al límite de respetar el pleno ejercicio de los derechos fundamentales de los titulares de los datos, como asimismo, a la obligación de consignar el nuevo dato que corresponda ante el pago de la deuda y su subsecuente eliminación, obligaciones que el Banco Estado de Chile no ha cumplido, al mantener en sus registros de deuda castigada aquella pagada por la actora el 23 de julio de 2018, no obstante estar en conocimiento de la transferencia electrónica realizada al Centro de Formación Técnica Santo Tomás por el mismo monto de la deuda castigada, según lo expresó al informar, y más aún, utilizando esa información como fundamento para desestimar la solicitud de la recurrente para acceder al sistema financiero, lo que constituye un acto arbitrario e ilegal que vulnera las garantías constitucionales consagradas en los números 2 y 24 del artículo 19 de la Carta Fundamental de la recurrente, puesto que le impide acceder a fuentes de financiamiento en términos de igualdad con otras personas, afectando consecuencialmente su patrimonio, en consideración al registros de datos que la recurrida mantiene internamente, sin ajustarse a las directrices y límites establecidos en la Ley N° 19.628" (CS, considerando 8º).
Nº 14.934-2020, 2 de junio de 2020. **Recurso de protección (rechazado)**	"La mantención de la deuda en el registro de morosidades, situación que se encuentra regulada en los artículos 18 y 19 de la Ley N° 19.628. En efecto, el inciso segundo del artículo 18 prohíbe en términos absolutos la mantención de la información, pero siempre que la obligación haya 'sido pagada' o que se haya 'extinguido por otro modo legal'. A su vez, el artículo 19 supedita el origen del deber de eliminar el dato al 'pago o extinción de la obligación'. Finalmente, el artículo 4° del Decreto Supremo N° 950 ya citado discurre en el mismo sentido, esto es, que la aclaración de una deuda solo procede respecto de obligaciones 'indudablemente pagadas o que se hubiesen extinguido de otro modo legal con posterioridad al protesto o a su publicación en el Boletín'. En resumen, únicamente el pago de la obligación o su 'extinción por otro modo legal' hacen aplicables las disposiciones de los artículos 18 inciso segundo y 19 de la Ley Nº 19.628" (CS, considerando 6º). Que, efectuadas las precisiones que anteceden, es manifiesto que solo la prescripción de la deuda produce los efectos extintivos a que se refieren el inciso 2° del artículo 18 y el artículo 19, ambos de la Ley N° 19.628, y el artículo 4° del Decreto Supremo N° 950, toda vez que la prescripción de la acción ejecutiva que emana del pagaré subsiste como ordinaria, conforme a lo dispuesto en el inciso segundo del artículo 2515 del Código Civil" (CS, considerando 8º).
Nº 33.187-2020, 10 de junio de 2020. **Recurso de protección (acogido)**	"Que, como lo ha resuelto antes esta Corte en los autos Roles N° 4.207-2019, 7.316-2019 y 7.299-2019, es preciso considerar 'que el artículo 13 bis de la Ley N° 19.848, introducido por la Ley N° 19.899, publicada en el Diario Oficial de 18 de agosto de 2003 (posterior a las Leyes N° 19.628 y 19.812) interpreta el artículo 15 inciso 2° de la Ley N° 19.287, en el sentido que las nóminas de los deudores morosos de los fondos solidarios de crédito universitario son públicas sin que les haya sido ni les sea aplicable lo establecido en la Ley N° 19.628, sobre Protección a la Vida Privada'" (CS, considerando 4°).

	"Que, no obstante lo expuesto anteriormente, el referido artículo 15 de la Ley N° 19.287 no faculta de modo alguno a hacer un cobro inoportuno, por el contrario éste debe ejercerse dentro de un plazo razonable, siendo del todo improcedente forzar como un medio alternativo al cobro judicial la publicación a través de los informes financieros y comerciales de empresas habilitadas a estos efectos, originando con este proceder un medio de cobro impropio" (CS, considerando 5°).
N° 32.337-2020, 29 de abril de 2020. **Recurso de protección (acogido)**	"Vulnera lo previsto en el artículo 6 de la ley 19.628, que dispone: 'Los datos personales deberán ser eliminados o cancelados cuando su almacenamiento carezca de fundamento legal o cuando hayan caducado', el banco que incluye en las nóminas que envía a la Comisión del Mercado Financiero, la información de que la actora registra una deuda con el recurrido, lo cual da cuenta que éste no desinformó la referida acreencia. Asimismo se infringe el artículo 19 de la ley 19.628, en tanto dispone: 'Al efectuarse el pago o extinguirse la obligación por otro modo en que intervenga directamente el acreedor, éste avisará tal hecho, a más tardar dentro de los siguientes siete días hábiles, al responsable del registro o banco de datos accesible al público que en su oportunidad comunicó el protesto o la morosidad, a fin de que consigne el nuevo dato que corresponda, previo pago de la tarifa si fuere procedente, con cargo al deudor'".
N° 24.469-2020, 10 de noviembre de 2020. **Recurso de protección (acogido)**	"El registro de deuda castigada al que hace referencia la institución financiera recurrida, se encuentra regido por la Ley N 19.628, por tratarse del almacenamiento, registro o banco de datos a los que se refieren sus artículos 1 y 2 y, por consiguiente, sujeto al límite de respetar el pleno ejercicio de los derechos fundamentales de los titulares de los datos, como asimismo, a la obligación de consignar el nuevo dato que corresponda ante el pago de la deuda y su subsecuente eliminación. Al mantener en sus registros de deuda castigada aquella pagada por la actora el 23 de julio de 2018, no obstante estar en conocimiento de la transferencia electrónica realizada al Centro de Formación Técnica Santo Tomás por el mismo monto de la deuda castigada, según lo expresó al informar, y más aún, utilizando esa información como fundamento para desestimar la solicitud de la recurrente para acceder al sistema financiero, lo que constituye un acto arbitrario e ilegal que vulnera las garantías constitucionales consagradas en los números 2 y 24 del artículo 19 de la Carta Fundamental de la recurrente, puesto que le impide acceder a fuentes de financiamiento en términos de igualdad con otras personas, afectando consecuencialmente su patrimonio, en consideración al registros de datos que la recurrida mantiene internamente, sin ajustarse a las directrices y límites establecidos en la Ley Nº 19.628".

Estándares internacionales de protección de datos personales

← Índice de contenidos

2.1 La protección de datos en Europa

Los derechos fundamentales del hombre no son más que la evolución de las ideas de libertad e igualdad lanzadas desde la antigua democracia griega, abriéndose paso hasta nuestros días a través de sucesivos avances y retrocesos, decía en sus clases el constitucionalista Pedro de Vega García.[24] En su largo camino hasta hoy, dichas ideas sufrieron múltiples avatares: se diversificaron, se adaptaron a nuevas realidades, evolucionaron en otros conceptos, se han contraído en ambientes dictatoriales y han vuelto a expandirse al calor de la discusión democrática.

Y no solo han evolucionado en su desarrollo, sino también en las formas que las sociedades los usan o entienden en determinados momentos, adaptándose a nuevos escenarios y necesidades.

Así por ejemplo, los derechos económicos, sociales y culturales se desplegaron cuando el hambre y la miseria campeaban en el ambiente de posguerra de Europa; el derecho a vivir en un medioambiente libre de contaminación cobró fuerza cuando las grandes ciudades se ahogaban con las emanaciones tóxicas de las industrias[25], y el derecho humanitario se despliega y toma sus formas características cuando los grandes desplazamientos humanos, azuzados por la catástrofe, revelaron su peor rostro.

Así también nació el derecho fundamental a la protección de datos personales, cuando la recogida, conservación y procesamiento de datos o información de personas identificadas o identificables durante la Segunda Guerra Mundial puso en jaque la vida y libertad de esas

24 Pedro de Vega García fue catedrático de Derecho Constitucional de la Universidad Complutense de Madrid hasta su fallecimiento en 2016. Discípulo y colaborador de Enrique Tierno Galván, estudió la tensión permanente entre constitucionalismo y democracia en *La Reforma Constitucional y la Problemática del Poder Constituyente* (Tecnos, Madrid, 1985), obra de referencia en materia de reforma constitucional.

25 Tómese como ejemplo la niebla que cubrió a Londres a fines de los años 1951 y 1952 y a principios de 1953, compuesta principalmente de hollín, dióxido de carbono y dióxido de azufre, causando muertes y enfermedades masivas, ayudado por las condiciones atmosféricas y el estacionamiento de las emanaciones tóxicas producidas por la misma ciudad.

personas. Más adelante, el desarrollo de las tecnologías permitió el procesamiento de la información (personal), aprovechándose estas potencialidades en la adopción de decisiones respecto de otros, quienes no pocas veces vieron que sus circunstancias se transformaban (usualmente para mal) porque *alguien*, tampoco es claro *quién*, había tomado una decisión a su respecto en base a *cierta información* (no sabían cuál) obtenidas de fuentes que no podían determinar.

Por supuesto, en tales circunstancias las personas tampoco estaban en condiciones de cuestionar la veracidad o la calidad de la información de fuente ignota, pero sufrían todos sus efectos: eran despedidos de sus trabajos, se les negaba el acceso a la compra o alquiler de viviendas, también el acceso a ciertas prestaciones de salud, y un largo etcétera de consecuencias indeseadas producidas por decisiones arbitrarias de quienes, en definitiva, tenían la capacidad de vulnerar todos y cada uno de los derechos de las personas que orgullosamente exhiben las Constituciones y las leyes.

¿Por qué ocurrió esto? Porque nuestro sistema de derecho continental europeo no tenía herramientas para proteger a las personas frente a un fenómeno nuevo y sin precedentes en la historia: el tratamiento automatizado de datos personales realizado en forma masiva y distribuida.

Efectivamente, algunas de las máquinas de tabulación de censos poblacionales habían sido utilizadas exitosamente en la persecución política y racial de la Alemania nazi[26], pero a partir de la década de los 80 las computadoras ya no eran herramientas accesibles solo al Estado o a la grandes universidades: se había iniciado la masificación de la capacidad de procesamiento de datos a gran escala y se abrían también, de par en par, las puertas a decisiones arbitrarias basadas en los datos que arrojaban las máquinas que los procesaban.

26 Existe una abundante literatura que documenta la colaboración entre el que fuera el principal proveedor de máquinas de tabulación, como lo fue la empresa IBM, y el régimen de Adolf Hitler, pero destacamos de entre ellas, como punto de partida, el libro *IBM y el Holocausto*, del historiador Edwin Black, publicado en castellano por la editorial Atlántida de Buenos Aires, en 2001.

Estos riesgos y amenazas fueron advertidas tempranamente y algunos países comenzaron a tomar ciertas providencias para cautelar los derechos de las personas o establecer límites a la actividad informática. El primero de ellos fue el Estado de Hesse, en la República Federal de Alemania, donde se dicta la *Datenschutzgesetz*, de 7 de octubre de 1970, una ley de 17 epígrafes que establece un marco al tratamiento de datos que realicen los organismos públicos y las personas jurídicas de derecho público (como la Universidad Goethe de Frankfurt am Main), y solo alcanza a las empresas privadas en la medida que realizan actuaciones delegadas por la administración pública.

Aparece aquí por primera vez la figura de una **autoridad de protección de datos**, el Supervisor de Protección de Datos de Hesse, elegido por el Parlamento e independiente del poder político, que informa anualmente el estado de avance en materias de protección de datos.[27]

Tres años más tarde, Suecia también dictó su propia ley, la *Datalag* (1973:289), que contemplaba la creación de un sistema público de registro de bases de datos, el establecimiento de una autoridad de protección de datos (*Datainspektionen*) y un extenso listado de **ilícitos** que incluye sanciones que van desde multas a prisión.

Ahora, ninguna de estas leyes contemplaba otorgar amplios derechos a los titulares de los datos, pero ambas son fruto del intenso debate político y académico abierto en la década de los 60 en Europa sobre si el procesamiento automatizado de datos por el Estado amenazaba el equilibrio de poder entre los ciudadanos y los gobiernos, que finalmente se tradujo en la Recomendación 509 de la Asamblea del Consejo de Europa, de 1968,"*relative aux droits de l'homme et aux réalisations scientifiques et technologiques modernes*". En ella se manifiesta la convicción de que las modernas tecnologías de recogida y procesamiento de la información "son una amenaza para los derechos y libertades de la persona y, en particular, el derecho al respeto de la vida privada", lo que en definitiva condujo al Comité de Ministros del

27 El primer supervisor fue Spiros Simitis, profesor de la Universidad Goethe, considerado el "padre" de la protección de datos en Alemania y quien posteriormente, entre 1982 y 1986, ocupó el cargo de Presidente de la Comisión de Expertos sobre Protección de Datos del Consejo de Europa.

Consejo de Europa a dictar resoluciones destinadas tanto a proteger los datos personales en el ámbito privado (1973) como en el ámbito público (1974).

La especial sensibilidad de la opinión pública a las técnicas de control social condujo a que, inmediatamente después de las legislaciones de Hesse y Suecia, siguieran ese camino legislativo Renania-Palatinado (1974), Francia (1978) y la República Federal de Alemania (1977), pero ninguna de ellas atisbó la existencia de un derecho fundamental nuevo subyacente a todas estas regulaciones legales.

Los estándares internacionales, si bien toman elementos comunes de estas primeras leyes, se han ido construyendo a partir de instrumentos de derechos humanos, debates en el seno de foros de carácter económico y organismos asociativos, integrados por autoridades de protección de datos personales. A ellos nos referiremos en las siguientes páginas.

Primeras leyes de protección de datos personales

Hesse, Alemania: *Datenschutzgesetz* (07.10.1970)	**Autoridad de protección de datos:** Supervisor de Protección de Datos de Hesse
Suecia: *Datalag*, 1973:289 (11.05.1973), derogada en 1998	**Autoridad de protección de datos:** *Datainspektionen*. Régimen infraccional: ilícitos de protección de datos.
Alemania: Ley Federal de Protección de Datos (27.01.1977)	**Autoridad de protección de datos:** Comisario Federal de protección de datos, además de reconocer la autoridad supervisora del *Lander*.
Francia: Ley sobre informática, ficheros y libertades (06.01.1978)	**Institucionalidad:** Comisión Nacional de Informática y Libertades (CNIL).

2.1.1 Convenio Nº 108 del Consejo de Europa, de 28 de enero de 1981

La discusión pública y el desarrollo supranacional de los conceptos y nociones asociadas al abuso del tratamiento de datos personales, decantó en que el Consejo de Europa tomara cartas en el asunto y adoptara su Convenio Nº 108, llamado "Convenio del Consejo de Europa, de 28 de Enero de 1981, para la Protección de las Personas

El Convenio Nº 108 tiene varias características que lo convierten, normativamente, en la piedra basal de la protección contra el uso inadecuado de los datos personales.

con respecto al Tratamiento Automatizado de Datos de Carácter Personal", el cual establece los principios esenciales, imperativos y vinculantes en la materia para otorgar protección jurídica a los individuos; este Convenio también tuvo un Protocolo Adicional[28], que es parte constitutivo del mismo y abordó especialmente lo referido a transferencia internacional de datos personales.

El Convenio Nº 108 tiene varias características que lo convierten, normativamente, en la piedra basal de la protección contra el uso inadecuado de los datos personales.

En primer lugar, tiene pretensiones de universalidad y ello se refleja en que aún hoy está abierto a la adhesión de los Estados que no son miembros del Consejo de Europa, pues se reconoce que el flujo de datos es transfronterizo. Incluso Chile podría adherir al Convenio, como ya lo ha hecho Uruguay.[29]

En segundo lugar, el Convenio Nº 108 y su Protocolo Adicional se aplican a todos los sectores de la sociedad: justicia, *retail*, telecomunicaciones, administración pública, seguros, comercio, salud, etcétera, incluso a las relaciones entre particulares ("sectores público y privado").

Y en tercer lugar, el Convenio señala principios a los que el tratamiento de datos personales está sujeto, pero indicando que la directriz es la ampliación de la protección de los derechos y de las libertades fundamentales de las personas, concretamente en lo referido al derecho al respeto de la vida privada; cuestión que, como ya veremos, varía más adelante cuando se entiende que la vida privada es solo uno más de los derechos que puede verse afectado por el inadecuado tratamiento de datos personales.

28 Nos referimos al "Protocolo Adicional de Convenio Nº 108 para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal y relativo a Transferencias de Datos", de 8 de noviembre de 2001.

29 Por Ley Nº 19.030, publicada el 7 de enero de 2013, de la República Oriental del Uruguay.

Junto con ciertas definiciones básicas, como entender dato personal como "cualquier información relativa a una persona física identificada o identificable", ordena a los Estados obligados por el Convenio a tomar las medidas necesarias para que hacer efectivos los principios básicos, que podemos sintetizar de la manera que sigue:

a. **Principio de lealtad y licitud.** Los datos personales deben obtenerse y tratarse de forma leal y legítima.

b. **Principio de finalidad.** Los datos personales solo pueden tratarse para finalidades determinadas y no pueden ser utilizados para fines diferentes a los que fueron recabados; cumplida su finalidad, deben eliminarse.

c. **Principio de necesariedad.** Los datos a tratar deben ser adecuados, pertinentes y no excesivos en relación con los fines.

d. **Principio de calidad.** Quienes realicen operaciones de tratamiento de datos son responsables de que estos sean exactos y que estén al día.

e. **Principio de seguridad.** Deben tomarse todas las providencias necesarias para evitar la destrucción accidental o no autorizada, la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizada de los datos personales.

Este modelo normativo, basado en el respeto de ciertos principios, marca el derrotero de la regulación en materia de protección de datos personales que se aplica hasta hoy.

También, el Convenio Nº 108 innovó al otorgarles a los titulares de los datos ciertos derechos, como son el derecho a conocer quiénes tenían sus datos (acceso), el derecho a rectificar el contenido de los mismos (rectificación), el derecho a solicitar el borrado de los mismos (cancelación) y el derecho a tener recursos efectivos que hicieran posible el ejercicio de los derechos.

Ahora, a pesar de que su texto es del año 1981, el Convenio Nº 108 del Consejo de Europa entró en vigencia general recién el 1 de octubre de 1985, y en ese intertanto ocurrieron cuestiones muy significativas que cambiaron la forma de comprender sus disposiciones, potenciando su importancia como texto normativo.

Países no europeos que han adherido al Convenio Nº 108

País	Ratificación	Entrada en vigor
Cabo Verde	19.06.2018	01.10.2018
Mauricio	17.06.2016	01.10.2016
México	28.06.2018	01.10.2018
Senegal	25.08.2016	01.12.2016
Uruguay	10.04.2013	01.08.2013

En este momento, se encuentra abierto a firma y ratificación el protocolo por el cual se moderniza el Convenio Nº 108, para adecuarlo a los nuevos desarrollos tecnológicos.[30]

2.1.2 El determinante fallo del Tribunal Constitucional Alemán en el caso de la Ley del Censo de 1983

Mientras el Convenio Nº 108 todavía buscaba adhesiones entre los países de Europa, el 4 de marzo de 1982 fue aprobado en la entonces República Federal de Alemania la ley del censo de población[31], censo que se realizaría el año siguiente (*Volkszählungsgesetz* 1983), lo que significó que durante ese año 1983 se expidieran por correo postal las preguntas del censo a todos los habitantes del país, para que estos las respondieran y las remitieran a la Oficina del Censo.

Sin embargo, a pesar de las promesas de que se trataba de un ejercicio anónimo en que la identidad de las personas que se encuestaban jamás sería revelada, muchas de ellas se negaron a contestar, pues el nivel

30 Tratado Nº 223, "Protocolo por el que se modifica el Convenio para la Protección de las Personas con respecto al Tratamiento Automático de Datos Personales" (CETS Nº 223), Estrasburgo, 10.10.2018, cuya entrada en vigor se encuentra prevista a la fecha de ratificación de todas las partes del tratado ETS Nº 108 o el 11 de octubre de 2023.

31 La Ley del Censo de Población de 1983 fue aprobada por el *Bundestag* el 4 de marzo de 1982 y se publicó el día 31 de ese mismo mes.

de detalle de las preguntas era tan invasivo que con ejercicios muy simples era posible asociar las respuestas del censo con la identidad de una persona determinada.

Ante la negativa a contestar, la oficina correspondiente cursó multas y algunos de los multados formularon una reclamación ante el Tribunal Constitucional el 5 de marzo de 1983, fundados en que a su parecer el censo, en la forma en que se presentaba, vulneraba el libre desenvolvimiento de la personalidad y la dignidad humana, como también la libertad de expresión y garantías de orden procesal.

Pero, como señalamos, en el ordenamiento jurídico de Alemania no existe la *Privacy* ni se la ha recogido; tampoco existe la intimidad en la Ley Fundamental (nombre oficial de la Constitución alemana), pero sí ampara la dignidad de la persona (1.1) y el libre desarrollo de la personalidad (2.1)[32], a partir de lo cual los jueces construyeron el "*Recht auf informationelle Selbstbestimmung*", esto es, el "derecho a la autodeterminación informativa", y que se trata de un derecho fundamental autónomo.[33]

Por tanto, la sentencia del Tribunal Constitucional de la República Federal de Alemania[34], dictada el 15 de diciembre de 1983 y que resolvió el asunto, declaró como violatorio de la Ley Fundamental algunos preceptos de la Ley del Censo de 1983[35], disparando con ello un proceso de reforma doctrinal, jurisprudencial y legislativa que llega hasta nuestros días.

32 "Todos tienen derecho al libre desarrollo de su personalidad en tanto en cuanto no lesione los derechos ajenos y no contravenga el orden constitucional o las buenas costumbres".

33 Debemos hacer presente aquí que, a este caso, no era aplicable el texto del ya mencionado Convenio Nº 108, del Consejo de Europa, pues si bien era conocido desde 1981, Alemania solo lo ratificó el 19 de junio de 1985, entrando en vigencia general para toda Europa a partir 1 de octubre de 1985, tras la ratificación o aprobación de Suecia, Francia, España, Noruega y, por último, la República Federal de Alemania.

34 Todos los fragmentos de la sentencia que en adelante reproduciremos corresponden a la traducción que hizo de la misma Manuel Daranas, la que fue publicada en el *Boletín de Jurisprudencia Constitucional* Nº 33 de las Cortes Generales, Madrid, 1984, pp. 126-170 (lo que se indique entre corchetes es de los autores).

35 Esta ley, aprobada por unanimidad y sin mayor debate por el *Bundestag*, compelía a responder a las más de 100 preguntas del censo poblacional correspondiente. Dada la entidad y cantidad de las interrogantes, algunos ciudadanos se negaron a responderlas, por lo que el Estado accionó contra ellos, con las consecuencias que se traducen en la referida sentencia.

La columna vertebral del razonamiento judicial es que el derecho al libre desarrollo de la personalidad, unido a la inviolable dignidad de las personas, sobreentiende la existencia de la facultad de los individuos de decidir por sí mismos las vías de divulgación y el tipo de uso que debe darse a los datos referentes a su propia persona y que las limitaciones a ese derecho solo pueden imponerse por ley, pero esas leyes solo serán constitucionalmente válidas si se fundan en un interés general superior.

El Tribunal Constitucional alemán entiende que la clave de bóveda del ordenamiento constitucional se encuentra en el valor de la libertad y la dignidad de la persona, quien tiene derecho a actuar con libre autodeterminación como miembro de una sociedad libre y por ello tiene la facultad "de decidir básicamente por sí mismo cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida".

Pero para que esa facultad no sea ilusoria, el tratamiento de datos personales requiere de medidas especiales de protección, dado que la "información individual sobre circunstancias personales u objetivas de una persona determinada o, en su caso, determinable, son técnicamente hablando acumulables sin límite alguno y en cualquier momento se pueden recabar en cuestión de segundos, cualquier que sea la distancia" y, más aún, esa información puede refundirse con otras colecciones de datos creando perfiles de personalidad ampliamente precisos, sin que el titular de los datos pueda controlar su exactitud y su utilización, dice el tribunal.

Señala también que las tecnologías han ensanchado en una medida no cuantificable las posibilidades de indagar e influir sobre la conducta del individuo, pues el que no pueda percibir con seguridad suficiente qué informaciones relativas a él son conocidas en determinados sectores de su entorno social puede verse sustancialmente cohibido en su libertad de planificar o decidir.

No es, entonces, compatible con el derecho a la autodeterminación informativa, un orden social y un orden jurídico que hiciese posible que el ciudadano no pueda saber quién, qué, cuándo y con qué motivo alguien sabe algo sobre él, pues "quien se siente inseguro

de si en todo momento se registran cualesquiera comportamientos divergentes y se catalogan, utilizan o transmiten permanentemente a título de información procurará no llamar la atención con esa clase de comportamiento. Quien sepa de antemano que su participación, por ejemplo, en una reunión o en una iniciativa cívica va a ser registrada por las autoridades y que podrán derivarse riesgos para él por este motivo renunciará presumiblemente a lo que supone un ejercicio de los correspondientes derechos fundamentales".

Lo anterior, a juicio del Tribunal Constitucional alemán, "no solo menoscabaría las oportunidades de desarrollo de la personalidad individual, sino también el bien público, porque la autodeterminación constituye una condición elemental de funcionamiento de toda comunidad fundada en la capacidad de obrar y de cooperación de sus ciudadanos".

Entonces, como corolario deduce lo siguiente: "La libre eclosión de la personalidad presupone en las condiciones modernas de la elaboración de datos la protección del individuo contra la recogida, el almacenamiento, la utilización y la transmisión ilimitadas de los datos concernientes a la persona" y este es un derecho fundamental.

Razona el sentenciador que el derecho a la autodeterminación informativa tiene límites, pues no es absoluto, dado que la personalidad de los individuos se desarrolla y desenvuelve dentro de una comunidad social a la cual se integra.

Continúa, el tribunal alemán, declarando que también es decisivo que exista una finalidad en el tratamiento de datos personales, sobre todo si se considera que no hay datos carentes en sí mismo de interés, pues gracias al procesamiento automatizado de datos, aquellos que aparentemente carecen de valor pueden ser relacionados con otros afectando la autodeterminación de los individuos, lo que trae como consecuencia que solo cuando se tenga clara la finalidad con la cual se piden los datos (del censo, en este caso, pero válido para cualquier otro supuesto) y qué posibles usos pueden dárseles "se podrá contestar la interrogante sobre la licitud de las restricciones del derecho a la autodeterminación informativa".

Entonces, "toda coerción al suministro de datos de referencia personal exige que el legislador haya determinado la finalidad de utilización con toda precisión en cuanto al *ámbito y que los datos sean adecuados y necesarios para esa finalidad*" y, en consecuencia, la recogida y acopio de datos para fines indeterminados o indeterminables son incompatiblescon el derecho a la autodeterminación informativa.

Dentro de esta lógica, el sentenciador señala que quienes recopilen datos no anonimizados para el cumplimiento de su respectiva misión deben limitarse al **mínimo indispensable para la consecución del objetivo indicado**, y ese mínimo se reduce al objetivo fijado por la ley [*finalidad*]. Si bien, entrando a la resolución del caso concreto, los jueces alemanes precisan que la recopilación de datos con fines estadísticos no requiere que cada uno de ellos esté vinculado con una finalidad.

Lo anterior, sin embargo, tampoco significa que quepa exigir aquí cualesquier tipo de datos, pues es un deber del legislador, aun cuando se trate de datos personales que van a usarse para fines estadísticos, comprobar si esos datos, respecto de los cuales ordenará facilitarlos, llevan o no aparejado el peligro de calificar socialmente al titular de los mismos (drogadicto, persona con antecedentes penales, enfermo mental, individuo asocial, etcétera) y debe evaluar si necesita realmente esa información o si podría conseguir la misma finalidad perseguida a través de otros medios menos gravosos para los derechos de la persona [*proporcionalidad*].

En palabras del tribunal, tan evidente es la vinculación de este derecho a la libertad y autodeterminación del individuo, que la sentencia entiende que la conducta de la persona podrá verse afectada severamente a través de su vulneración. Así, la sentencia sostiene que:

> "El que [*la persona*] no pueda percibir con seguridad suficiente qué informaciones relativas a él son conocidas en determinados sectores de su entorno social y quien de alguna manera no sea capaz de aquilatar lo que puedan saber de él sus posibles comunicantes puede verse sustancialmente cohibido en su libertad de planificar o decidir por autodeterminación (…). Quien se siente inseguro de si en todo momento se registran cualesquiera comportamientos

> divergentes y se catalogan, utilizan o transmiten permanentemente a título de información, procurará no llamar la atención con esa clase de comportamiento. Quien sepa de antemano que su participación, por ejemplo, en una reunión o iniciativa cívica va a ser registrada por las autoridades y que podrán derivarse riesgos para él por este motivo, renunciará presumiblemente a lo que supone un ejercicio de los correspondientes derechos fundamentales (…) esto no solo menoscabaría las oportunidades de desarrollo de la personalidad individual, sino también el bien público, porque la autodeterminación constituye una condición elemental de funcionamiento de toda comunidad fundada en la capacidad de obrar y de cooperación de los ciudadanos".

Finalmente, razonan los jueces que la coerción estatal, como las multas, solo son eficaces en una medida muy mínima, pues toda actuación del Estado que burle los intereses de los ciudadanos puede resultar ventajosa a corto plazo, pero a la larga conduce a una reducción de la cantidad y exactitud de la información que proporcionen los ya desconfiados ciudadanos.

La autodeterminación informativa es el derecho del individuo a controlar la obtención, tenencia, tratamiento y transmisión de datos relativos a su persona, decidiendo en cuanto a los mismos las condiciones en que dichas operaciones pueden llevarse a cabo.

Concluyen los juzgadores, en síntesis, señalando que algunos párrafos de la Ley del Censo de 1983 son incompatibles con el derecho general a la personalidad y la protección de la dignidad humana contemplados en el art. 2° y 1° de la Ley Fundamental, respectivamente, declarando la nulidad de las mismas.

Entonces ¿qué es en sí la autodeterminación informativa?

La autodeterminación informativa es el derecho del individuo a controlar la obtención, tenencia, tratamiento y transmisión de datos relativos a su persona, decidiendo en cuanto a los mismos las condiciones en que dichas operaciones pueden llevarse a cabo. Se trata de controlar la utilización de las informaciones personales independientemente si estas pueden ser calificadas de íntimas, reservadas, secretas, privadas: no es relevante su mayor o menor proximidad con el ámbito o núcleo íntimo de las personas.

2.1.3 Directiva 95/46/CE, del Parlamento Europeo y del Consejo de 24 de octubre de 1995

Diez años después de la entrada en vigencia del Convenio Nº 108, se aprobó la "Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 2015, 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"[36], que vino a actualizar, ampliar y redireccionar los contenidos del citado Convenio, sobre todo en consideración de las disparidades legislativas que se habían producido en los Estados nacionales.

Esta vez, el derecho a proteger no es la "vida privada", como se decía en el Convenio Nº 108, sino que ahora el consenso parece apuntar al "derecho a la intimidad", pero de una forma no exclusiva ni excluyente de los demás derechos fundamentales.

Ahora bien, se debe tener presente que a pesar de que las declaraciones de la Directiva 95/46/CE nos recuerdan que "los sistemas de tratamiento de datos están al servicio del hombre", y que no basta garantizar la libre circulación de los datos personales de un Estado a otro sino también la protección de los derechos fundamentales de las personas, la verdad es que se trata de una norma de ordenamiento legislativo del mercado comunitario, destinada a crear en los Estados nacionales una legislación más o menos estandarizada y con una institucionalidad equivalente, que garantice o dé lugar a un tratamiento similar al tema de protección de datos para efectos de hacer posible la libre circulación de la información relativa a las personas dentro del mercado europeo.

Es decir, más que un desarrollo jurídico de carácter doctrinario, se trata de reglas dirigidas a los Estado integrantes de la entonces Comunidad Europea, a fin de asentar de mejor forma un mercado común basado en reglas lo más uniformes posibles, y casi todos los considerandos de la Directiva recuerdan a los "socios" el proceso en que están involucrados y las cuestiones que deben respetarse, como

36 Esta Directiva, elaborada en Luxemburgo, fue publicada en el Diario Oficial de las Comunidades Europeas el 23 de noviembre de 1995.

es el caso de la prohibición de transferir datos a terceros países que no ofrezcan un nivel de protección adecuado respecto de los datos personales de los europeos.

Parte la Directiva complementando algunas definiciones ausentes en el Convenio, como el concepto de tratamiento de datos personales, que entiende como "cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción", amplitud que el concepto mantiene hasta nuestro días, como pudimos ver al referirnos a la definición contenida en nuestra Ley Nº 19.628.

También se ocupa de definir que el objeto regulado es la **base de datos personales**[37], entendida como "todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica".

Los estándares de protección de datos en la Directiva 95/46/CE los visualizamos en la consagración de los principios de protección de datos, los que perfila y ordena en torno a dos metaprincipios: los relativos a la **calidad de los datos** y los que conciernen a la **legitimación para realizar tratamiento** de ellos.

En su artículo 12, expresa la existencia del derecho de acceso, esto es, de obtener del responsable del tratamiento de datos, libremente, sin restricciones y con una periodicidad razonable y sin retrasos ni gastos excesivos, la información relativa a si se están tratando datos que conciernen a la persona, de qué datos se trata y la lógica que subyace al tratamiento de los mismos. Extrañamente, también con-

37 En realidad, la Directiva 95/46/CE no habla de "bases de datos" sino de "ficheros de datos personales", pero dados los términos de la definición y la escasa aplicación del término "fichero" en Chile, para una mejor comprensión usaremos en su lugar la expresión "bases de datos".

templa la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajusta a la Directiva, pero no entiende que sean derechos diferentes al de acceso.

En su artículo 14, la Directiva contempla un importante avance: el derecho de oposición del interesado o titular de los datos a que aquellos que le conciernan sean objeto de tratamiento, salvo cuando la legislación nacional disponga otra cosa.

De igual modo, se obliga a los Estados a crear recursos judiciales y administrativos para los casos de violación de derechos aplicables al tratamiento de datos, lo que va unido también a la obligación del responsable del tratamiento de reparar los perjuicios sufrido por el titular de ellos como consecuencia de las infracciones que cometa [*tutela judicial efectiva*].

Se reitera también la idea del Convenio Nº 108 y su Protocolo Adicional, en el sentido de que no se puede transferir libremente los dados de los individuos de los Estados miembros a terceros Estados, salvo que una evaluación demuestre que el tratamiento de datos en ese tercer país cumple con las normas europeas.

Finalmente, se establece que los Estados necesariamente deben contar con una autoridad de protección de datos, con potestades de investigación y poderes de intervención que lo habiliten a ordenar el bloqueo, supresión y destrucción de datos e incluso prohibir su tratamiento, teniendo además capacidad procesal para actuar ante los tribunales de justicia [*institucionalidad independiente, técnica y con facultades suficientes*].

Como señalamos, la Directiva 95/46/CE fue sustituida por el "Reglamento (UE) 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 y por el que se deroga la Directiva 95/46/CE", que entró en vigor el 25 de mayo de 2018, por lo que pierde sentido ahondar en el contenido de la Directiva, si bien no está de más destacar alguno de sus principales efectos: la estandarización internacional de conceptos y principios a los que nos hemos refe-

rido, que han sobrevivido como plenamente válidos hasta hoy, y la influencia de estos, que incluso fueron recogidos prácticamente en su totalidad en nuestra vigente Ley Nº 19.628, de 1999, sobre protección de la vida privada.

2.1.4 Reglamento General de Protección de Datos (RGPD), de 25 de mayo de 2018, como estándar de facto para la interpretación de la protección de datos personales en Chile

La medianoche del 24 de mayo de 2018, los principios, derechos y normas relativos a protección de datos personales se volvieron a barajar con efectos globales, con ocasión de la entrada en vigencia del que hemos citado como reglamento europeo o RGPD, pero cuyo nombre oficial completo es: "Reglamento (UE) 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 y por el que se deroga la Directiva 95/46/CE".

Es importante que la denominación "Reglamento" no llame a error, pues no se trata de potestades normativas del Poder Ejecutivo, sino que, en la nomenclatura del derecho comunitario europeo, los reglamentos son actos legislativos vinculantes que deben aplicarse en su integridad en toda la Unión Europea. Es decir, rigen directamente al interior de los países de la Unión, a diferencia de las Directivas, que son actos legislativos en los cuales se establecen objetivos que todos los países deben cumplir, pero donde le corresponde a cada uno de ellos elaborar sus propias leyes para alcanzar dichos objetivos (modelos de leyes o leyes modelo).

También es necesario no errar en otro aspecto: a pesar de que parece aplicarse solo a Europa, en realidad tiene un alcance global que lo lleva a tener impactos concretos incluso en los países más alejados de ese continente, como el nuestro, tanto por la influencia de la normativa y el desarrollo de la protección de datos como derecho fundamental en todo el orbe, como también por normas que afectan las relaciones contractuales y comerciales de quienes se relacionan, directa o indirectamente, con productos y servicios que fluyen hacia el Viejo Continente o que provienen del mismo; es decir, el Reglamento

introdujo reglas de aplicación extraterritorial que afectan a entidades ubicadas fuera de la Unión Europea[38], las que incluso pueden quedar sujetas a su régimen sancionador, que no se caracteriza precisamente por su laxitud.

Si bien el Reglamento cambia, en los hechos, los estándares internacionalmente aplicables a los datos personales, no lo hace a través de cambios revolucionarios, sino más bien a través de una reformulación de lo ya existente.

Así, los principios establecidos por el Reglamento desde el año 2018, en relación al tratamiento de datos, imponen que los datos personales sean tratados de manera lícita, leal y transparente en relación con el interesado ("**licitud, lealtad y transparencia**"); que deben ser recogidos con fines determinados, explícitos y legítimos, no pudiendo ser tratados de manera incompatible con dichos fines ("**limitación de la finalidad**"); que deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados ("**minimización de datos**"), y que deben ser exactos y, de ser necesario, actualizados ("**calidad**").

Además, establece por principio que los datos solo pueden ser mantenidos durante el tiempo necesario para el cumplimiento de sus fines ("**limitación del plazo de conservación**" o "temporalidad"); que deben ser tratados de tal manera que se garantice su seguridad, integridad y confidencialidad ("**integridad y confidencialidad**"), y finalmente, que el responsable del tratamiento debe ser capaz de demostrar que ha cumplido cabalmente con las responsabilidades que el Reglamento le impone ("**responsabilidad proactiva**", "**responsabilidad demostrada**", **"protección de datos desde el diseño**"). A vía ejemplar, el Tribunal de Justicia de la Unión Europea falló al respecto que el responsable del tratamiento de datos debe ser capaz de demostrar que el titular de los datos otorgó su consentimiento ex-

38 Solo a manera de ejemplo, citamos este fragmento del art. 3 del RGPD: "El presente Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, **independientemente de que el tratamiento tenga lugar en la Unión o no**".

preso, libre, informado e inequívoco para la conservación de la cédula de identidad de los clientes en sus bases de datos, y que no cumple este requisito el sistema que prellena la casilla de consentimiento.[39]

Adicionalmente, el Reglamento se refiere a la institucionalidad, a cuyo respecto exige que sea autónoma, integrada en redes de colaboración internacionales ("**coordinación y colaboración**"), estableciendo derechos de los titulares ("**tutela efectiva**").

En materia de transferencia internacional de datos personales, el RGPD dispone que la transferencia a un país tercero solo puede llevarse a cabo, en principio, si el país tercero en cuestión garantiza un nivel de protección adecuado a los datos personales, correspondiéndole a la Comisión [*europea*] hacer constar que un país de fuera de la Unión cuenta con legislación interna o compromisos internacionales que cumplan con este requisito.[40]

Como podemos ver, salvo por reemplazos terminológicos y reagrupación de conceptos, los cambios no son sustanciales y tampoco contradictorios, sino que más bien responden a una evolución y desarrollo normativo enriquecido con la madurez y experiencia que dan las nuevas realidades que se presentan en el mundo, frente a la evidencia del desarrollo tecnológico en materia de tratamiento de datos personales.

Por supuesto, el Reglamento jamás asume que el derecho a la protección de datos sea absoluto, sino que, por el contrario, señala que pueden existir limitaciones al mismo, aunque declara expresamente en su artículo 85 que "Los Estados miembros **conciliarán** por ley el derecho a la protección de los datos personales en virtud del presente Reglamento con el derecho a la libertad de expresión y de información, incluido el tratamiento con fines periodísticos y fines de expresión académica, artística o literaria".

39 STJUE, C-61/19, de 11.11.2020: Orange Romania SA y Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal (ANSPDCP). Disponible en línea [consulta: 02.02.2021].

40 Al respecto, véase: "El Tribunal de Justicia invalida la Decisión 2016/1250 sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU" (europa.eu). Disponible en línea [consulta: 02.02.2021].

2.2 Estándares de protección de datos personales de la OCDE (2002)[41]

En un intento por establecer estándares en materia de protección de datos personales, en el seno del Consejo de la OCDE se acordaron las directrices sobre protección de la privacidad y flujos transfronterizos de datos personales, también conocidas como "directrices de privacidad", las cuales pretenden tener aplicación general a todos los ámbitos y tanto en la legislación interna como internacional, además de su aplicación a la legislación formal como a la autorregulación. Los principios que se consideran en este caso son los siguientes:

- Principio de **limitación de recogida**: considera que debieran establecerse limitaciones para la recogida de datos personales y, en cualquier caso, la obligación de que los datos se deban obtener con medios legales y justos y, siempre que sea apropiado, con el conocimiento o consentimiento del afectado (titular de los datos).
- Principio de **calidad de los datos**: los datos personales que sean objeto de tratamiento deben ser relevantes en relación a la finalidad para la cual son tratados, además de ser exactos, completos y actualizados.
- Principio de **especificación del propósito**: la finalidad del tratamiento de datos debe especificarse a más tardar a la época de la recogida y su tratamiento se limitará al cumplimiento de la finalidad legítima e informada o a finalidades compatibles con esta, especificando en cada momento el cambio de objetivo.
- Principio de **limitación de uso**: los usos de los datos quedan limitados por la finalidad legítima e informada, salvo que exista el consentimiento del afectado o haya mediado autorización legal o de la autoridad competente.

41 Ver resumen disponible en línea [consulta: 02.02.2021].

— Principio de **salvaguardia de la seguridad**: se adoptarán las medidas razonables para proteger los datos personales contra riesgos tales como pérdidas, accesos o usos no autorizados, destrucción, modificación o divulgación de los mismos.

— Principio de **transparencia**: se deberán establecer políticas generales en relación a la evolución, prácticas y políticas de tratamiento de datos, además de contar con medios ágiles para determinar la existencia y la naturaleza de los datos personales, el propósito principal para su uso y la identidad y lugar de residencia habitual del controlador de los datos (responsable del tratamiento).

— Principio de **participación individual**: se debe establecer el derecho de la persona a que el responsable le confirme si tiene datos de su persona, en un tiempo razonable, a un precio accesible, no excesivo, de forma razonable e inteligible; que se explique de manera razonable la razón por la cual estas solicitudes podrían ser denegadas; las vías de impugnación, y el derecho a expresar dudas sobre el tratamiento que se efectúa de sus datos, solicitar que se eliminen, rectifiquen, completen o corrijan aquellos que le conciernen. Asimismo, los países deben "brindar los medios razonables para que los individuos ejerzan sus derechos".

— Principio de **responsabilidad**: sobre todo responsable de su tratamiento debe recaer la responsabilidad del cumplimiento de las medidas que hagan efectivos los principios antes señalados.

Adicionalmente, se prevén algunas directrices generales para los Estados, a saber:

— **Restricciones al libre flujo internacional de datos personales y legitimidad**: Los países deben adoptar las medidas que aseguren un flujo transfronterizo de datos personales de manera ininterrumpida y segura, por lo que podrá negarse la transferencia internacional de datos a países mientras el país destinatario no observe de forma sustancial las directrices de tratamiento de datos o cuando algunas categorías de datos personales tienen regulaciones especiales que no son equiparables a las que rigen en el país de destino de los datos.

— **Cooperación internacional**: Se prevé que los países informen de manera regular las medidas que han adoptado para dar cumplimiento a las directrices, además de establecer mecanismos de colaboración en cuestiones procesales y de investigación.

2.3 Principios en materia de protección de datos personales en la Resolución de Madrid (2009)

A partir de la adopción de la Directiva 95/46/CE, se fue conformando una activa colaboración de diversas autoridades de protección de datos de distintos países del mundo. En el marco de la labor de estas redes de colaboración, en la 31ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, celebrada el 5 de noviembre de 2009 en Madrid, se acordó una propuesta conjunta para la redacción de estándares internacionales en relación con el tratamiento de datos de carácter personal, documento conocido como "Estándares Internacionales sobre Protección de Datos Personales y Privacidad", o Resolución de Madrid, o simplemente Estándares de Madrid.

Los Estándares de Madrid tienen el mérito de dar a entender, en un lenguaje claro y sencillo, el contenido y la manera en que los principios y derechos de la Directiva 95/46/CE debían regularse e interpretarse en las diversas legislaciones del mundo.

Así, el primer principio o punto de partida es el **principio general de legitimación**, esto es, que como regla general los datos de carácter personal solo pueden ser tratados previa obtención del consentimiento libre, inequívoco e informado del titular de los mismos (el "interesado", en términos de la Resolución de Madrid), o cuando un interés legítimo de la persona que realiza el tratamiento (el "responsable") justifique dicha operación, salvo que prevalezcan los intereses, derechos y libertades de los titulares; también se entiende legitimado el tratamiento de datos que sea necesario para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular (los contratos de suministro, por ejemplo, en que se debe saber a quién hay que prestarle determinado servicio y cobrarle por ello).

También se está liberado de obtener el consentimiento del titular de los datos cuando el tratamiento de los mismos sea necesario para el cumplimiento de una obligación impuesta por ley, o que emane del legítimo ejercicio de las competencias de un organismo de la administración pública o cuando concurran situaciones excepcionales

que pongan en peligro la vida, la salud o la seguridad del titular o interesado o de otra persona, como podría ser el caso de la necesidad de acceder al historial médico de quien ha resultado herido que no puede darse a entender y es necesario comprobar que no es alérgico a determinado medicamento que pretenda suministrársele.

Sintetizando, conforme al principio general de legitimación, el tratamiento de datos personales solo puede llevarse a cabo si existe el consentimiento del titular de los datos o si una ley lo autoriza. Si bien podrá haber diversas circunstancias que se enmarquen en una u otra de estas legitimantes, no hay más.[42]

El segundo principio (enumerado de esta forma solo con fines de ordenación y no de relevancia o jerarquía) es el **principio de lealtad y legalidad**, el cual implica que los tratamientos de datos de carácter personal se deberán realizar de manera leal [*de buena fe*], conforme a la legislación nacional y respetando los derechos y libertades de las personas [*legalidad*].

La Resolución de Madrid nos aclara que deben ser considerados desleales aquellos tratamientos de datos y carácter personal que den lugar a discriminaciones injustas o arbitrarias respecto de la persona.

El tercer principio que se reconoce en los Estándares de Madrid es el **principio de finalidad**, que impone que el tratamiento de datos de carácter personal deberá limitarse al cumplimiento de las finalidades explicitadas al titular de los datos al momento de solicitarle el consentimiento, o las que prevea la ley.[43] Por ende, el responsable del tratamiento no podrá llevar a cabo tratamientos incompatibles con las finalidades para las que hubiese recabado los datos de carácter personal, salvo que cuente con el consentimiento inequívoco y específico del interesado, sin que basten declaraciones genéricas.

42 En ese mismo sentido, el artículo 4° de la Ley N° 19.628 de 1999 señala: "El tratamiento de los datos personales solo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello".

43 La Ley N° 19.628 lo recoge en los siguientes términos: "Artículo 9°. Los datos personales deben utilizarse solo para los fines para los cuales hubieren sido recolectados, salvo que provengan o se hayan recolectado de fuentes accesibles al público".

Otro factor que autorizaría el tratamiento fuera de la finalidad originalmente considerada dice relación con la fuente de los datos, en el sentido de que será legítimo su tratamiento si constan en fuentes de libre acceso al público, pero no hay novedad en este caso, porque la fuente legitimante, en este caso, es la ley.

El cuarto es el **principio de proporcionalidad**, que para las autoridades de protección de datos implica que el tratamiento de datos de carácter personal deberá circunscribirse a aquéllos que resulten adecuados, relevantes y no excesivos en relación con las finalidades previstas, por lo que los responsables del tratamiento deberán realizar esfuerzos razonables para limitar los datos de carácter personal tratados al mínimo necesario [*minimización de datos*].

Existe un quinto, el **principio de calidad**, que tiene dos implicancias distintas. Por una parte, significa que los responsables del tratamiento de datos deberán asegurar en todo momento que los datos de carácter personal sean exactos, así como que se mantengan tan completos y actualizados como sea necesario para el cumplimiento de las finalidades para las que sean tratados. Y por otra, que se debe limitar al mínimo necesario el periodo de conservación de los datos de carácter personal tratados para satisfacer la finalidad del tratamiento. En los términos de nuestra legislación nacional, "la información debe ser exacta, actualizada y responder con veracidad a la situación real del titular de los datos".[44]

Así, si los datos de carácter personal han dejado de ser necesarios para el cumplimiento de las finalidades que legitimaron su tratamiento, deberán ser eliminados o convertidos en anónimos [*disociados-anonimizados*].

El sexto principio en esta enumeración es el **principio de transparencia**, en virtud del cual toda persona responsable de tratamientos de datos personales deberá contar con políticas transparentes en lo que a ello se refiere y, además, deberá facilitar a los interesados, esto

44 Art. 9° de la Ley N°19.628 de 1999, sobre protección de la vida privada.

es a los titulares de los datos personales, la información acerca de la identidad del responsable del banco de datos, 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 o titulares podrán ejercer los derechos de acceso, rectificación, cancelación o eliminación y oposición (que veremos con más detalle más adelante), así como cualquier otra información necesaria para garantizar el tratamiento leal de dichos datos de carácter personal.

¿Cuándo se debe proporcionar esta información? De acuerdo a la Resolución de Madrid, si los datos de carácter personal han sido obtenidos directamente del titular, la información deberá ser facilitada en el momento de la recogida, de lo contrario deberá ser facilitada en un plazo prudencial de tiempo. Asimismo, se prevé que en aquellos casos que el cumplimiento de este requisito resulte imposible o exija un esfuerzo desproporcionado, pueda realizarse a través de medidas alternativas tales como avisos en diarios de circulación nacional.

En todo caso, la información que da paso al consentimiento no puede limitarse a la firma de una cláusula perdida entre los términos de un farragoso contrato-tipo, sino que la información deberá facilitarse empleando para ello un lenguaje claro y sencillo.

Ahora bien, si los datos de carácter personal son recogidos en línea a través de redes de comunicaciones electrónicas, las obligaciones de transparencia podrán satisfacerse mediante la publicación de políticas de protección de datos fácilmente accesibles e identificables.

El séptimo y último elemento de esta enumeración es el **principio de responsabilidad**, que implica que quienes tratan datos personales de terceros deben adoptar las medidas necesarias para cumplir con los principios y normas de la legislación y dotarse de aquellos mecanismos necesarios para evidenciar dicho cumplimiento, tanto ante los titulares de datos como ante las autoridades competentes. Es decir, no basta con afirmar que se cumple la ley, sino que se debe estar en condiciones de demostrarlo [*responsabilidad demostrable*].

Finalmente la Resolución de Madrid le dedica un acápite especial al tema de la seguridad, señalando que quienes realizan operaciones de tratamiento de datos personales tienen dos importantes deberes respecto de sus operaciones.

Uno de ellos es el **deber de seguridad**, que entiende como el deber de proteger los datos de carácter personal que se sometan a tratamiento mediante las medidas técnicas y organizativas que resulten idóneas en cada momento para garantizar la integridad, confidencialidad y disponibilidad de la información.

Esto deriva del hecho que los responsables realizan operaciones de riesgo, con posibles consecuencias negativas para los titulares de los datos, agravadas por el hecho de que muchos de los datos pueden ser de carácter sensible, lo que los obliga a poner especial cuidado en el estado de la técnica y del contexto en el que se efectúa el tratamiento, así como de las obligaciones establecidas en las leyes.

Este deber de seguridad implica también el informar a los titulares de datos de cualquier infracción de seguridad que pudiese afectar sus derechos patrimoniales o extrapatrimoniales, así como de las medidas adoptadas para su solución. Asimismo, conlleva por parte del responsable el **deber de confidencialidad**, esto es, que quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal deberán respetar la confidencialidad de los mismos, obligación que subsistirá aun después de finalizar sus relaciones con el interesado.[45]

De nuestra parte, sostenemos que todos estos principios señalados están presentes en la ley chilena, aunque no todos hayan sido formulados en forma literal, sino que la mayoría de ellos se encuentran implícitos en la regulación.

De nuestra parte, sostenemos que todos estos principios señalados están presentes en la ley chilena, aunque no todos hayan sido formulados en forma literal, sino que la mayoría de ellos se encuentran implícitos en la regulación.

45 Este deber está considerado en el artículo 7° de la Ley N° 19.628: "Las personas que trabajan en el tratamiento de datos personales, tanto en organismos públicos como privados, están obligadas a guardar secreto sobre los mismos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público, como asimismo sobre los demás datos y antecedentes relacionados con el banco de datos, obligación que no cesa por haber terminado sus actividades en ese campo".

Así por ejemplo, cuando la ley habla de que "el tratamiento de datos personales por parte de un organismo público solo podrá efectuarse respecto de las materias de su competencia y con sujeción a las reglas precedentes", en realidad está aplicando el principio general de legitimación; y cuando dice que "el responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños", está hablando del principio de responsabilidad.

2.4 Estándares de protección de datos personales para los Estados iberoamericanos (OEA, 2016)[46]

Como ya se señaló, los estándares contenidos en la Resolución de Madrid datan de 2009, pero en el año 2016 se acordó, en el marco de la XXV Cumbre Iberoamericana de Jefes de Estado y Gobierno[47], solicitar a la Red Iberoamericana de Protección de Datos (RIPD)[48] la elaboración de una propuesta de trabajo para facilitar la cooperación entre países en materia de protección de los datos personales.

Como respuesta a este requerimiento la RIPD presentó al año siguiente, en Santiago de Chile, el documento "Estándares de Protección de Datos Personales para los Estados Iberoamericanos", que persigue esencialmente establecer un conjunto de principios y derechos comunes de protección de datos personales que los Estados iberoamericanos puedan adoptar y desarrollar en su legislación nacional, con la finalidad de contar con reglas homogéneas en la región.

Por supuesto, este documento no se elaboró desde cero, sino que para construirlo la RIPD declara haber tenido a la vista diversos instrumentos internacionales dictados con anterioridad, entre ellos, el Reglamento General de Protección de Datos de Europa, que todavía no entraba en vigor, pero que ya había sido aprobado en 2016.

En cuanto a su contenido, los principios que recomienda incorporar en las iniciativas legislativas de los países iberoamericanos son los mismos de la Resolución de Madrid, ya revisados, esto es legitimación, transparencia, finalidad, calidad, proporcionalidad, responsabilidad, pero con un par de innovaciones.

46 Véase OEA: Departamento de Derecho Internacional (DDI) Protección de Datos Personales (oas.org). Disponible en línea [consulta: 12.09.2021].

47 Véanse al respecto los documentos emanados de la XXV Cumbre Iberoamericana de Jefes de Estado y de Gobierno. Disponibles en línea [consulta: 15.10.2020].

48 La Red Iberoamericana de Protección de Datos (RIPD), creada en 2003, es un foro para la integración de quienes desarrollan iniciativas y proyectos relacionados con la protección de datos personales, tanto del sector público como en el privado, en Iberoamérica.

La primera de ellas es que el principio de lealtad y legalidad lo divide en *lealtad*, entendida como la proscripción de tratar datos personales a través de medios engañosos y fraudulentos, o que de ello resulten discriminaciones arbitrarias para sus titulares; y *licitud*, como la obligación de quienes tratan datos personales de sujetarse al derecho interno, destacando particularmente que las autoridades públicas, en materia de datos personales, solo pueden hacer lo que las normas le autoricen expresamente.

La segunda innovación de la RIPD es que la seguridad y la confidencialidad ya no los considera solo como deberes que deben incorporarse en la regulación legislativa que se haga en la materia por los respectivos Estados, sino que establece que también deben ser considerados principios basales, entendiendo que el principio de seguridad supone establecer las medidas administrativas, físicas y técnicas suficientes para garantizar la confidencialidad, integridad y disponibilidad de los datos personales, y que el principio de confidencialidad obliga a incorporar en las legislaciones nacionales mecanismos de control para asegurar la confidencialidad de la información.

Adicionalmente, se contienen algunas directrices orientadoras que, en opinión de la Red iberoamericana de Protección de Datos (RIPD), pueden justificar limitaciones al derecho a la protección de datos personales: seguridad nacional, seguridad pública, protección de la salud pública, la protección de los derechos y libertades de terceros y, también, cuestiones de interés público, todas las cuales deben ser establecidas expresamente en la ley, siguiendo en esto lo señalado por la sentencia del Tribunal Constitucional alemán en 1983.

Lo anterior no significa abrogar el derecho a la protección de datos personales, sino un ejercicio intelectual más delicado, como es el camino de **conciliar** dicho derecho con otros derechos y libertades:

de acuerdo a los Estándares iberoamericanos no es aceptable sencillamente hacerlo desaparecer en determinados supuestos legales, sino que requiere un ejercicio de ponderación.[49]

49 El numeral 7 de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos, señala: "Ponderación del derecho a la protección de datos personales. 7.1. Los Estados Iberoamericanos podrán exentar, en su derecho interno, el cumplimiento de los principios y derechos previstos en los presentes Estándares, exclusivamente en la medida en que resulte necesario conciliar el derecho a la protección de datos personales con otros derechos y libertades fundamentales. 7.2. Esta exención deberá requerir de un ejercicio de ponderación con la finalidad de determinar la necesidad, idoneidad y proporcionalidad de la restricción o excepción conforme a las reglas y criterios que establezcan los Estados Iberoamericanos en su derecho interno".

2.5 Acuerdo de Asociación entre la Comunidad Europea y Chile y sus efectos en materia de protección de datos personales

Hemos mencionado bastante el Reglamento General de Protección de Datos de la Unión Europea (RGPD), por lo que resulta legítimo preguntarse cuál es la razón de relevarlo si, en principio, no tiene aplicación en nuestro país.

La respuesta que nos relaciona con dicho reglamento es doble. Por una parte, las empresas y universidades europeas regidas por este cuerpo normativo, cuando celebran contratos y/o convenios con entidades chilenas, normalmente introducen en el texto del acuerdo la obligación de realizar operaciones de tratamiento de datos en condiciones similares a como se hacen en la Unión Europea (lo que eventualmente llegará a tribunales chilenas en razón de incumplimiento de contratos). Y por otra, nuestro país suscribió un tratado internacional vigente llamado "Acuerdo por el que se establece una Asociación entre la Comunidad Europea y sus Estados miembros, por una parte, y la República de Chile, por otra"[50], que señala textualmente en su artículo 202: "Las Partes acuerdan otorgar un elevado nivel de protección al procesamiento de datos personales y de otra índole, compatible con las más altas normas internacionales".

¿Cuál es la más alta norma internacional en la materia? El Reglamento General de Protección de Datos, que entró a regir el 25 de mayo de 2018, aplicable directamente a Europa y exigible a los países que han obtenido el reconocimiento de país con un nivel adecuado de protección de datos, como lo son Argentina, Canadá, Israel, Japón, Nueva Zelanda y Uruguay; es decir, a partir de 2018 los estándares deben buscarse en la lectura del Reglamento, pues ese es el acuerdo de nuestro país con la Comunidad Europea, hoy Unión Europea.

50 Decreto N° 28 de 2003, del Ministerio de Relaciones Exteriores, publicado en el Diario Oficial el 1 de febrero de 2003.

¿Por qué razones llegarían a conocer los tribunales nacionales cuestionessobre aplicación del RGPD de Europa?

Por litigios sobre responsabilidad por incumplimiento de contratos, cuando una de las partes se hubiere comprometido a cumplir estándares europeos en materia de protección de datos.	Por causas judiciales en las que se discuta el auténtico sentido y alcance de los principios y normas de la Ley Nº 19.628, en cuanto a estándares exigibles al tratamiento de datos personales.

Todos estos textos, sean o no normativos, nos ilustran respecto a la interpretación de lo que actualmente nos es exigible como país en materia de protección de datos personales.

Probablemente, a estas alturas cabe preguntarse también qué tiene que ver este panorama de principios, como la Resolución de Madrid de 2009, los Estándares de Protección de Datos Personales para los Estados Iberoamericanos de 2017 y el Reglamento General de Protección de Datos de 2018, con la realidad legislativa de Chile.

La respuesta es que todos estos textos, sean o no normativos, nos ilustran respecto a la interpretación de lo que actualmente nos es exigible como país en materia de protección de datos personales. Consideremos que la legislación interna de Chile fue dictada en 1999 y, en los hechos, tiene como antecedente la Directiva 46/95 de Europa.

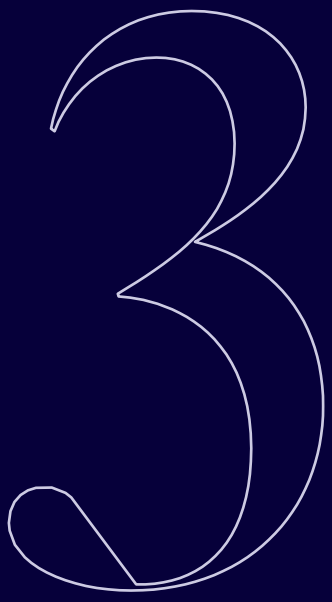
Ya hemos visto que, en líneas generales, nuestra Ley Nº 19.628 cumple con las exigencias de la Resolución de Madrid, si bien nos faltan algunas cosas que se asentaron en los Estándares Iberoamericanos y algunas otras que se consignan en el Reglamento General de Protección de Datos.

A continuación se presenta un cuadro síntesis de los principios, conforme a su establecimiento en cada uno de los instrumentos analizados.

Principios de tratamiento de datos personales

Principio	Convenio Nº 108	RGPD Europa	Estándares OCDE	Estándares de Madrid	Estándares OEA
Lealtad y licitud	X	X		X	X
Finalidad, limitación de la finalidad, especificación del propósito	X	X	X	X	X

Necesariedad, minimización de datos, proporcionalidad	X	X	X	X	
Calidad, calidad de datos, protección de datos desde el diseño	X	X	X	X	X
Seguridad, salvaguardia de la seguridad	X	X	X		X
Temporalidad, limitación del plazo de conservación		X			
Responsabilidad, responsabilidad proactiva, responsabilidad demostrada		X	X	X	
Tutela efectiva, participación individual		X	X		X
Coordinación, colaboración		X	X		
Transparencia información, consentimiento		X	X		X



El desarrollo normativo de la protección de datos en Chile

← Índice de contenidos

Ya nos hemos referido a que la Ley Nº 19.628 se gestó a partir de una moción parlamentaria y que Chile, en el año 2018, reconoció la protección de datos personales como un derecho fundamental. Actualmente, el artículo 19 Nº 4 garantiza "el derecho al respeto o protección de la vida privada y la honra de las personas y su familia y la protección de datos personales", con lo cual se reconoce la diferenciación entre lo que es la protección de datos personales y el derecho a la protección de la vida privada.

Como ya se señaló, si bien la ley se tituló "Ley sobre protección de la vida privada" de acuerdo a lo previsto en el proyecto de ley en tramitación, pasaría a denominarse "Regula el tratamiento de datos personales".

En este capítulo, analizaremos la evolución de la normativa nacional desde que el 28 de agosto de 1999 se publicara en el Diario Oficial la Ley Nº 19.628, luego de haber concluido un largo proceso legislativo iniciado en 1994.

Como ya se señaló, si bien la ley se tituló "Ley sobre protección de la vida privada" de acuerdo a lo previsto en el proyecto de ley en tramitación, pasaría a denominarse "Regula el tratamiento de datos personales". Con ello se iba a corregir el error de circunscribir la ley solo a la protección de la vida privada, en circunstancias de que protege todas las esferas de la persona respecto del tratamiento que terceros hagan de la información que le concierne.

3.1 La reforma constitucional de 2018

Empujado por la tendencia internacional, en 2018 se reconoció como garantía fundamental en la Constitución de la República de Chile el derecho a la protección de datos personales.[51] El texto original propuesto fue el siguiente:

51 El proyecto de ley se inició por moción de los senadores Hernán Larraín Fernández, Felipe Harboe Bascuñán, Eugenio Tuma Zedán, Pedro Araya Guerrero y Ricardo Lagos Weber, con fecha 11 de junio de 2014 (Boletín Nº 9384-07), como un intento de adecuar nuestra carta de derechos a los derechos de tercera generación, consistente en la facultad de la persona de controlar sus datos personales y la capacidad para disponer y decidir sobre los mismos.

"Toda persona tiene derecho a la protección de sus datos personales y obtener su rectificación, complementación y cancelación, si estos fueran erróneos o afectasen sus derechos, como asimismo a manifestar su oposición, de acuerdo con las disposiciones establecidas en la ley. Su tratamiento solo podrá hacerse por ley o con el consentimiento expreso del titular".

En el proyecto se reconoce que a esa época, "en el ámbito de los países latinoamericanos destaca la normativa colombiana, que consagra este derecho en el inciso segundo del artículo 15 de su Carta Fundamental (promulgada en 1991); la Constitución de Ecuador, establece en su artículo 92 una acción de habeas data con rango constitucional, y la Constitución Mexicana, que consagra en su artículo 16 la protección de los datos personales y los derechos de acceso, rectificación, cancelación y oposición, derechos incorporados a la Constitución en junio del año 2009. Finalmente, hacen mención que normativas similares se han establecido en la Constitución de la República Federal de Brasil (1988) y en la de Paraguay (1992)".[52]

Adicionalmente, en 2005 Perú había incorporado en su Constitución el artículo 2.6, que garantiza a toda persona el "derecho a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar", Ecuador ya en 1998 había incorporado el artículo 94 que prevé que "toda persona tendrá derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su propósito", por mencionar algunos de los países que ya habían avanzado en esta materia en nuestro entorno.

Durante la tramitación, en nuestro país, Pablo Olmedo manifestó que ya el Tribunal Constitucional había reconocido que la "Carta Fundamental contiene un garantía implícita de protección de datos personales, tal como manifestó en los roles acumulados 1732 y 1800; y 1990 (Recurso de inaplicabilidad por inconstitucionalidad contra

52 Historia de la ley, p. 8.

el artículo décimo, letra h) de la ley Nº 20.285, sobre acceso a la información pública, que incide en el reclamo de ilegalidad 'Televisión Nacional de Chile con Consejo para la Transparencia' rol Nº 945-2010, Corte de Apelaciones de Santiago; y Recurso de inaplicabilidad por inconstitucionalidad contra el inc. 2° del art. 5° y la letra b) del N° 1° del art. 21, ambos de la ley N° 20.285 que incide en el reclamo de ilegalidad caratulado 'Dirección Nacional del Servicio Civil con Consejo para la Transparencia' rol N° 541-2011, Corte de Apelaciones de Santiago, respectivamente), lo que supone que el titular de dichos datos tendría prerrogativas sobre el control de la información que le empece, y que el Consejo para la Transparencia en principio es la institución que podría dilucidar la procedencia de este derecho a la luz de la pugna entre la protección de datos personales y el acceso a la información pública en ejecución de su competencia".[53]

Finalmente, el texto aprobado a través de la Ley Nº 21.096, dispone: "Artículo único. Agrégase, en el numeral 4° del artículo 19 de la Constitución Política de la República, a continuación de la expresión 'y su familia', lo siguiente: ', y asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley'". Con ello, en el texto resultante de la Constitución quedó redactado en los términos siguientes:

> "4º. El respeto y protección a la vida privada y a la honra de la persona y su familia, y asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley".

Conforme se estimó en su momento, uno de los beneficios de la consagración de esta garantía dice relación con que el artículo 19 Nº 4 queda bajo el ámbito de acción del recurso de protección, sin embargo, en los hechos, esto no se ha traducido en una mayor cobertura del derecho. A vía ejemplar, en fallo dictado en autos rol Nº 6777-2019, de 27 de marzo de 2019, la Corte Suprema confirmó la

53 Historia de la ley, p. 9.

sentencia dictada por la Corte de Apelaciones de Santiago en causa rol Nº 15245-2019, donde se declara inadmisible la acción de protección interpuesta por cuanto "el recurso de protección tiene por objeto restablecer el imperio del derecho cuando este ha sido quebrantado por actos u omisiones arbitrarias o ilegales que amenazan, perturban o privan del ejercicio legítimo de alguna de las garantías que taxativamente numeradas en el artículo 20 de la Constitución Política de la República, dejando a salvo las demás acciones legales", por lo que considera que esta acción constitucional no es la vía idónea para impetrar la protección del derecho a la protección de datos personales.

Asimismo, como veremos al referirnos al derecho de cancelación, la Corte Suprema, en la primera época de vigencia de la reforma, negó de manera persistente el derecho de la persona a que se supriman o cancelen (olviden) sus datos personales en distintas plataformas digitales. Véase al respecto las siguientes sentencias de la Corte Suprema: rol Nº 28.480-2018; rol Nº 11.746-2017, y rol Nº 19.134-2018.

En cambio, en autos 31354-2018, la Corte Suprema revocó la sentencia de Corte de Apelaciones de Santiago que había declarado inadmisible el recurso de protección, decidiendo su admisibilidad. En dicho caso se invocaba asimismo el "derecho al olvido", esto es, el derecho de cancelación o supresión de datos, si bien luego el peticionario se desistió de la acción, por lo que es factible evaluar, a través de este caso, la efectividad de la acción.

Sin embargo, a partir de 2020 hemos advertido una modificación en la tendencia. A continuación se presenta tabla de síntesis de fallos que van en la línea de reconocer y proteger este derecho:

Rol	Acción	Fundamento	Norma aplicada
Nº 112.543-2020	Apelación en recurso de protección	Parcialmente acogido. La Corte estima que la comunicación de deudas derivadas de financiamiento universitario es arbitraria e ilegal.	CPR: art. 19 Nº 4 y Nº 12. Ley Nº 19.628: arts. 1º, 2º, 4º y 17 inc. 2. Ley General de Bancos: art. 14.

Nº 132.263-2020	Apelación en recurso de protección	Acogido. La Corte estima que es arbitrario e ilegal realizar una transmisión en vivo desde el domicilio del recurrente sin su consentimiento y sin otorgar oportunidad de respuesta o contra argumentación.	CPR: art. 19 Nº 4. Ley Nº 19.628: art. 2º letra f. DL Nº 799 de 1974.
Nº 138.566-2020	Apelación en recurso de protección	Acogido. Constituye un acto arbitrario e ilegal el poner a disposición de terceros la imagen de una persona, asociada al calificativo de "acoso sexual" sin existir fundamento alguno.	CPR: art. 19 Nº 4. Ley Nº 19.628: art. 2º letra f.
Nº 21.137-2020	Apelación en recurso de protección	Acogido. Fondo Nacional de Salud incurre en un acto arbitrario e ilegal al sancionar al médico por no entregar las fichas clínicas de sus pacientes. Fonasa solo tiene atribución para tratar datos sensibles con el consentimiento del titular de los datos o para verificar otorgamiento de beneficios, y no para comprobar si un prestador ha infringido la legislación. El médico deberá proporcionar los datos básicos de sus pacientes para que dicha información sea actualizada por Compin.	CPR: art. 19 Nº 4, Nº 6 y Nº 24. Ley Nº 19.628: arts. 2º letra f y 10. Ley Nº 20.584. DFL 1 2005 Ministerio de Salud.
Nº 28.190-2019	Recurso de queja	Acogido. La Corte de Apelaciones incurre en falta o abuso grave al rechazar reclamo de ilegalidad contra decisión de amparo dictada por el Consejo para la Transparencia, que ordena al Ejército de Chile entregar información sobre dotación de las Fuerzas Armadas.	CPR: Art. 19 Nº. 4. Ley Nº 19.628: art. 4º. Ley Nº 20.050 de reforma constitucional. Ley Nº 20.285.

3.2 La Ley Nº 19.628 de 1999 y sus modificaciones

La Ley Nº 19.628 ha sido objeto de sucesivas modificaciones, la mayoría de ellas como reacción ante situaciones de abuso o en las cuales su texto ha resultado insuficiente. La mayoría de las modificaciones dicen relación con el tratamiento de datos de carácter económico y en este apartado nos referiremos a algunas de ellas.

En primer lugar, nos detendremos en la **Ley Nº 19.812**, también llamada "**ley Dicom**", que buscó hacer efectiva la garantía constitucional de "la libertad de trabajo y su protección", en uno de sus pilares, cual es el derecho a la no discriminación, que "prohíbe cualquiera discriminación que no se base en la capacidad o idoneidad personal, sin perjuicio de que la ley pueda exigir la nacionalidad chilena o límites de edad para determinados casos".

Esta ley, además de modificar la Ley Nº 19.628, introdujo un nuevo inciso sexto al artículo Nº 2 del Código del Trabajo, que consagra el **principio de no discriminación**, del siguiente tenor: "Ningún empleador podrá condicionar la contratación de trabajadores a la ausencia de obligaciones de carácter económico, financiero, bancario o comercial, que, conforme a la ley, puedan ser comunicadas por los responsables de registros o bancos de datos personales; no exigir para dicho fin declaración ni certificado alguno".

En lo que respecta a la Ley Nº 19.628, la Ley Nº 19.812 modificó los artículos 16, 17 y 18. En lo sustantivo, estableció una prohibición de comunicar datos personales que sean tratados en virtud del artículo 17 cuando se refieran a obligaciones que a la fecha de publicación de la ley hayan sido pagadas o se hayan extinguido por otro modo legal, así como los datos relativos a esas obligaciones que se hayan hecho exigibles antes del 1 de mayo de 2002 y se encuentren impagas, siempre que el total de obligaciones impagas del titular que comunique el registro o banco de datos a la fecha de publicación de la ley sea inferior a 2 millones de pesos por concepto de capital, excluyendo intereses, reajustes y cualquier otro rubro.

Asimismo, dispuso la eliminación de los datos relativos a créditos del Instituto Nacional de Desarrollo Agropecuario a sus usuarios, así como los datos relativos a deudas de personas que, al 30 de septiembre de 1999, obtuvieron créditos en el marco del programa de créditos para establecimiento por cuenta propia de chilenos retornados y que hayan optado, dentro del plazo establecido, a los beneficios que les otorga la Ley Nº 10.740, una vez aclarada la morosidad y previa solicitud.

Se agrega, en el inciso segundo del artículo 17, la prohibición de comunicar "la información relacionada con las deudas contraídas con empresas públicas o privadas que proporcionen servicios de electricidad, agua, teléfono y gas".

Finalmente, sustituyó los incisos primero y segundo del artículo 18 a efectos de prohibir la comunicación de datos relativos a morosidades y que se relacionen con una persona identificada o identificable, luego de transcurridos cinco años desde que la respectiva obligación se hizo exigible, como de aquellos relativos a las obligaciones que se hayan pagado o extinguido a través de otro modo legal.

Además de conocerse como ley Dicom, se reconoce porque perfecciona la ley en materia de **responsabilidad**, atendido que en el artículo 16 se incrementa asimismo la multa por la falta de entrega oportuna de la información en el derecho de acceso, o el retardo en efectuar la modificación solicitada en el derecho de rectificación, quedando en definitiva en un rango de 2 a 50 Unidades Tributarias Mensuales y, si el responsable del banco de datos requerido fuere un organismo público, establece como sanción al jefe de servicio la suspensión de su cargo por un lapso de 5 a 15 días.

Modificaciones introducidas por la Ley Nº 19.812
No discriminación: prohibición de discriminación en el acceso al empleo.
Temporalidad: 5 años desde que la deuda se hizo exigible.
Responsabilidad: multas de 2 a 50 UTM.
Proporcionalidad: impide comunicación de deudas con empresas de servicios básicos y créditos de retornados, así como de deudas que se hayan extinguido por alguna vía legal.

Más tarde, la **Ley N° 19.899**, publicada en el Diario Oficial el 18 de agosto de 2003, dispuso en su artículo 13 bis que "las nóminas de los deudores morosos de los fondos solidarios de crédito universitario son públicas sin que les haya sido ni les sea aplicable lo establecido en la Ley N° 19.812".

En su historia fidedigna, se señala que la ley permite publicar íntegramente la nómina de deudores morosos, modificando las normas aprobadas por el Congreso en la llamada ley Dicom, que consignaban limitaciones respecto de cuáles deudas podían darse a conocer y cuáles no.

En la dictación de la ley se tuvo a la vista lo resuelto por los tribunales en causa rol Nº C-10998-2006, de 25 de octubre de 2007, del 23º Juzgado Civil de Santiago y en autos rol Nº C-4505-2007, de 12 de mayo de 2009, del 24º Juzgado Civil de Santiago, todas dictadas a favor de Dicom.

De acuerdo al diario de sesiones de la Cámara de Diputados, en sesión del 13 de agosto de 2004, se buscaba que a las deudas por este tipo de obligaciones no se les aplicara la prohibición de publicarlas cuando hubieran cumplido el plazo que señala la ley que regula las morosidades, sino que se siguieran publicando las listas de estos deudores hasta que se extinga su deuda, dadas las condiciones favorables para los deudores previstas por el legislador en este tipo de créditos.

Modificación introducida por la Ley Nº 19.899
Permite la comunicación de la morosidad de deudas de crédito universitario.

A poco andar, se reconoció que los empleadores no respetaban lo previsto en el Código del Trabajo y que solicitaban un "informe Dicom" a las personas que postulan a un trabajo, desechando aquellas que presentaban información adversa. Por lo anterior, la **Ley Nº 20.463**, de 2010, modificó el artículo 17 de la Ley Nº 19.628, suspendiendo la comunicación de la información comercial de las personas cesantes. Los nuevos incisos incorporados disponen:

"Las entidades responsables que administren bancos de datos personales no podrán publicar o comunicar la información referida en el presente artículo, en especial los protestos y morosidades contenidas en él, cuando éstas se hayan originado durante el período de cesantía que afecte al deudor.

Para estos efectos, la Administradora de Fondos de Cesantía comunicará los datos de sus beneficiarios al Boletín de Informaciones Comerciales solo mientras subsistan sus beneficios para los efectos de que éste bloquee la información concerniente a tales personas.

Sin embargo, las personas que no estén incorporadas al seguro de cesantía deberán acreditar dicha condición ante el Boletín de Informaciones Comerciales, acompañando el finiquito extendido en forma legal o, si existiese controversia, con el acta de comparecencia ante la Inspección del Trabajo, para los efectos de impetrar este derecho por tres meses renovable por una vez. Para que opere dicha renovación se deberá adjuntar una declaración jurada del deudor en la que manifieste que mantiene su condición de cesante.

El bloqueo de datos será sin costo para el deudor.

No procederá el bloqueo de datos respecto de quienes consignen anotaciones en el sistema de información comercial durante el año anterior a la fecha de término de su relación laboral.

Las entidades responsables de la administración de bancos de datos personales no podrán señalar bajo ninguna circunstancia, signo o caracterización que la persona se encuentra beneficiada por esta ley".

Modificación introducida por la Ley Nº 20.463

Prohíbe la comunicación de información sobre morosidades de personas cesantes.

Luego, la **Ley Nº 20.591,** de 23 de julio de 2011, modificó el artículo 9º de la Ley Nº 19.628, introduciéndole el siguiente inciso final: "Prohíbese la realización de todo tipo de predicciones o evaluaciones de riesgo comercial que no estén basadas únicamente en información objetiva relativa a las morosidades o protestos de las personas naturales o jurídicas de las cuales se informa. La infracción a esta prohibición obligará a la eliminación inmediata de dicha información por parte del responsable de la base de datos y dará lugar a la indemnización de perjuicios que corresponda".

Esta modificación obedeció a una iniciativa parlamentaria gatillada por un hecho social, consistente en que se advirtió el uso del factor "consultas de tercero" en el cálculo del ranking de una persona determinada, información que no resultaría idónea porque depende de un factor totalmente ajeno a la persona, que incluso puede ser manipulado al antojo de quienes quisieran perjudicar a alguien. Además de lo anterior, los autores de la moción adujeron que la información sobre número de consultas no es información proveniente de fuente accesible al público y, por ende, para su tratamiento requiere de la autorización del titular de los datos personales.

En síntesis, los argumentos de los autores del proyecto de ley se refirieron a tres aspectos específicos, provenientes de la aplicación de los principios de **lealtad** y **licitud** en el tratamiento de datos personales, respecto de este instrumento de evaluación de riesgo comercial:

a. **Falta de calidad de la información**: porque se trataría de información no objetiva, ni originada en un hecho propio del titular del dato personal, sino más bien información generada a partir de una acción de un tercero, que es quien efectúa la consulta al RUT de la persona.

b. **Falta de calidad en el proceso**: por cuanto el dato "consulta al RUT"[54] no es información proveniente de una base de datos de libre acceso al público y, por ende, para su tratamiento se requiere la autorización del titular del dato personal, que en este caso es la persona cuyo RUT ha sido consultado.

54 El RUT corresponde al número de identificación a efectos tributarios.

c. **Afectación ilegítima a los derechos de los consumidores**: a este respecto, se dijo que la inclusión de la consulta al RUT de una persona le impedía a esta realizar acciones legítimas, tales como la cotización de un crédito en distintas entidades financieras, por cuanto cada una de las entidades cotizadas realiza la correspondiente evaluación de riesgo, afectando involuntariamente el ranking de la persona.

Otro factor relevante fue un fallo recaído en autos rol Nº 3937-2010, en que la Corte de Apelaciones de Santiago consideró que el *predictor de riesgo* de la recurrida (Equifax) vulneraba las garantías constitucionales consagradas en los números 2, 4 y 26 del artículo 19 de la Carta Fundamental, para luego sostener que "no obstante la conciencia de estos sentenciadores en cuanto al efecto relativo de las sentencias, no puede omitir el dejar constancia de su parecer en el sentido de que resultan tan obvias las ilegalidades y arbitrariedades que comete la recurrida, con la elaboración y puesta a disposición del público del denominado 'predictor de riesgo', que estiman se trata de una práctica a la que debiera ponerse término, para evitar así el poder llegar a dañar injustamente el crédito y la imagen de las personas, sin que exista autorización legal que lo permita, ni razones objetivas que lo avalen".

De nuestra parte, consideramos que la norma aprobada es perfectible, puesto que en su afán de limitar el uso de los *predictores* legitimó una nueva categoría de datos personales: los "**datos personales apreciativos**", esto es, aquellos que corresponden a una construcción realizada por un tercero distinto del titular de los datos, a partir de la información relativa a una persona y a través de una fórmula elaborada por dicho tercero, en base a los siguientes elementos:

- la elección del tipo de información a incluir en la base de cálculo,
- la determinación del factor a aplicar a cada tipo de información utilizada, y
- reglas de procesamiento (algoritmos).

Otro problema de la norma en comento dice relación con la inclusión de las personas jurídicas, en circunstancias de que la Ley Nº 19.628, en su ámbito de aplicación, solo incluye a las personas naturales.

Hasta ese momento, en Chile no se había regulado especialmente los datos apreciativos y, tal como advirtió la Corte de Apelaciones en el caso reseñado, debía considerarse que este tipo de datos carecía de fundamento legal y por tanto no quedaba amparado por el principio de licitud.

Otro problema de la norma en comento dice relación con la inclusión de las personas jurídicas, en circunstancias de que la Ley Nº 19.628, en su ámbito de aplicación, solo incluye a las personas naturales.

La Corte Suprema, en autos rol Nº 16852-2018, apelación de recurso de protección, consideró lo siguiente:

> "Como ya lo ha expresado reiterada y uniformemente esta Corte con anterioridad en los autos Roles Nos. 6.337-2014, 11.627-2014, 565-2015, 27.163-2015 y 68.681-2016, con arreglo a lo dispuesto por la letra f del artículo 2º de la citada ley [19.628], se entenderá por datos de carácter personal 'los relativos a cualquier información concerniente a personas naturales, identificadas o identificables.
>
> Luego, su letra g) añade que datos sensibles son aquellos que "se refieren 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".

A eso añade que la letra ñ del artículo 2° dispone que "para los efectosde esta ley se entenderá por: ñ) Titular de datos, la persona naturala la que se refieren los datos de carácter personal".

Por tanto, la Corte estima que las normas de la Ley Nº 19.628 no se aplican respecto de las personas jurídicas, reiterando lo ya resuelto por ese mismo tribunal en sentencias roles N° 4949-2012, Nº 68881-2016 y N° 2204-2018, entre otras.

Sin embargo, en otro fallo, dictado en autos rol Nº 27.889-2017, la Corte Suprema, en fallo de mayoría, acoge el recurso de protección interpuesto por una empresa [*persona jurídica*] por la publicación en Dicom de una morosidad que no constaba en alguno de los instru-

mentos previstos en el artículo 17 de la Ley Nº 19.628. Sin perjuicio de lo anterior, los votos de minoría de este caso se ajustan a lo que señalamos antes, en cuanto a que la Ley Nº 19.628 no tiene aplicación tratándose de datos de personas jurídicas.

En todo caso, si miramos la experiencia comparada, podemos sostener que efectivamente la construcción de estos indicadores debe responder a los principios generales y normas que rigen el tratamiento de datos personales.

Modificación introducida por la Ley Nº 20.591

Impone una norma imperativa de requisitos: que los predictores de riesgo comercial se elaboren a partir de **información objetiva relativa a las morosidades o protestos** de la persona natural o jurídica respecto de la cual se informa.

Finalmente, hay dos leyes que no podemos dejar de mencionar por su trascendencia en la materia que nos ocupa. En primer lugar la **Ley Nº 20.285**, de transparencia y acceso a la información pública, en tanto radica en el Consejo para la Transparencia el deber de velar por el cumplimiento de la Ley Nº 19.628 en los organismos públicos.

En segundo lugar, la **Ley Nº 20.575,** de 17 de febrero de 2012, sobre el principio de finalidad en el tratamiento de datos personales de que trata el Título III de la Ley Nº 19.628.

Esta ley, en su artículo 3º, dispone que "los responsables de los bancos de datos y los distribuidores de los registros o bancos de datos personales a que se refiere la ley [*esto es los sujetos a los que la ley los autoriza para realizar 'tratamiento de datos personales de carácter económico, financiero, bancario o comercial a que se refiere el Título III de la ley N° 19.628, sobre Protección de la Vida Privada'*], deberán, en el desarrollo de su actividad, implementar los principios de legitimidad, acceso y oposición, información, calidad de los datos, finalidad, proporcionalidad, transparencia, no discriminación, limitación de uso y seguridad en el tratamiento de datos personales, cuestión que deberá ser con-

siderada por el juez como un antecedente para determinar si existió la debida diligencia en el tratamiento de datos personales respetarse el principio de finalidad en el tratamiento de datos personales".

Adicionalmente, el artículo 4º impone la obligación de los distribuidores de los registros o bancos de datos personales de carácter económico, financiero, bancario o comercial, a "designar a una persona natural encargada del tratamiento de datos, de manera que los titulares de datos puedan acudir ante él para los efectos de hacer efectivos los derechos que les reconoce la Ley N° 19.628, sobre Protección de la Vida Privada".

En consecuencia, las nuevas obligaciones establecidas para este grupo objetivo son las siguientes:

a. Obligación de **designar un responsable** del tratamiento de datos personales.

b. **Limitación de uso** mediante la restricción del acceso a los datos sobre morosidades al comercio establecido y a las entidades que participan de la evaluación de riesgo comercial, quienes podrán utilizarlos en la evaluación de este riesgo comercial, eliminando el acceso universal a estos datos. Como podemos apreciar las limitaciones son en dos órdenes:

   — en primer lugar, se elimina el acceso universal a este tipo de información, por la vía de limitar el tipo de sujetos que puede acceder a ella; y

   — estos sujetos solo pueden utilizarla en las actividades calificadas por el legislador.

c. Crea la figura del **Distribuidor de Información Económica** (Dicom, SIISA, Sinacofi, Boletín Comercial, TU, etcétera).

d. **Obligación de implementar los principios** del tratamiento de datos personales. Si bien, calidad, finalidad, temporalidad, pertinencia y los demás principios que enuncia la ley no son una novedad en Chile, la gran diferencia es que se expresa la voluntad política de generar mecanismos eficientes de cumplimiento de dichas obligaciones.

Finalmente, ahondando en esta nueva visión del tratamiento de datos personales relativo a morosidades, el legislador establece las siguientes prohibiciones:

- Se prohíbe usar protestos y morosidades para procesos de selección de personal.
- Asimismo se prohíbe su uso para admisión en un establecimiento educacional, cualquiera sea el nivel y naturaleza pública o privada del establecimiento.
- Se prohíbe el uso de la misma en la solicitud de atención médica de urgencia.
- Tampoco podrá usarse en la evaluación de postulantes a cargos públicos.

3.3 La protección de datosy las leyes procesales

La Ley Nº 19.628 no excluye *a priori* el tratamiento de datos personales efectuado en el marco de las leyes procesales. En efecto, la única exclusión que se observa en el artículo 1º de esta ley refiere al tratamiento de datos que se efectúe en ejercicio de las libertades de emitir opinión y de informar, el que se regulará por la ley a que se refiere el artículo 19 Nº 12 de la Constitución Política de la República.

Luego, el artículo 21 de la Ley Nº 19.628 se refiere a los organismos públicos que sometan a tratamiento de datos la información relativa a condenas por delitos, infracciones administrativas o faltas disciplinarias, previendo que "no podrán comunicarlos una vez prescrita la acción penal o administrativa o cumplida o prescrita la sanción o la pena". Sin embargo, la exclusión no es absoluta por cuanto el inciso segundo de este mismo artículo dispone que se exceptúan "los casos en que esa información les sea solicitada por los tribunales de justicia u otros organismos públicos dentro del ámbito de su competencia, quienes deberán guardar respecto de ella la debida reserva o secreto y, en todo caso, les será aplicable lo dispuesto en los artículos 5º, 7º, 11 y 18, esto es, las reglas de comunicación electrónica de datos" (art. 5º), conforme al cual estos organismos podrán comunicar datos personales a través de métodos automatizados, en los términos siguientes:

> "Siempre que se cautelen los derechos de los titulares y la transmisión guarde relación con las tareas y finalidades de los organismos participantes".
>
> Luego, dispone que "frente a un requerimiento de datos personales mediante una red electrónica, deberá dejarse constancia de:
>
> a. La individualización del requirente;
>
> b. El motivo y el propósito del requerimiento, y
>
> c. El tipo de datos que se transmiten.

> La admisibilidad del requerimiento será evaluada por el responsable del banco de datos que lo recibe, pero la responsabilidad por dicha petición será de quien la haga.
>
> El receptor solo puede utilizar los datos personales para los fines que motivaron la transmisión.
>
> No se aplicará este artículo cuando se trate de datos personales accesibles al público en general.
>
> Esta disposición tampoco es aplicable cuando se transmiten datos personales a organizaciones internacionales en cumplimiento de lo dispuesto en los tratados y convenios vigentes".

El artículo 7º se refiere al **deber de secreto de las personas** que trabajen con los datos personales y el artículo 11 establece el **deber de cuidado y responsabilidad** por los datos personales.

La Ley Nº 20.886, que modifica el Código de Procedimiento Civil para establecer la tramitación digital de los procedimientos judiciales, en su artículo 2º letra c párrafo tercero dispone: "Se prohíbe el tratamiento masivo de los datos personales contenidos en el sistema de tramitación electrónica del Poder Judicial, sin su autorización previa. La infracción cometida por entes públicos y privados a lo dispuesto en este inciso será sancionada conforme a la Ley Nº 19.628".

Esta norma pretendía evitar la bajada masiva de la base de datos del Poder Judicial, lo que podría generar graves afectaciones al derecho a la protección de datos, sin embargo ha presentado inconvenientes desde otros aspectos, tales como el desarrollo de aplicaciones denominadas "*legaltech*" en general, antes llamadas "informática jurídica", así como los motores de vigilancia de juicios en particular, los cuales, para poder operar, requieren del consentimiento del administrador del sistema del Poder Judicial. Con todo, la norma nada dice respecto de solicitar la autorización del titular de los datos personales.

Otra cuestión relevante en este ámbito es determinar quién es la autoridad competente para otorgar el respectivo consentimiento, la Corporación Administrativa del Poder Judicial como administrador de esta base de datos, o la Corte Suprema como máxima autoridad jurisdiccional.

Un aspecto llamativo es que la norma aluda a un régimen infraccional supuestamente radicado en la Ley Nº 19.628, pero que no es tal, puesto que este es precisamente uno de los aspectos en los que la actual legislación se encuentra al debe en relación a los estándares internacionales en la materia.

No obstante, en la historia de la ley podemos advertir que, en el segundo informe de la Comisión de Constitución, se consigna que la Dirección de Estudios de la Corte Suprema propuso un texto que buscaba corregir estos aspectos, agregando en la parte final de la letra c, del siguiente tenor: "Se prohíbe a toda persona el tratamiento de los datos personales contenidos en el sistema de tramitación electrónica del Poder Judicial, sin autorización judicial previa. Asimismo, se establecerán medidas para evitar el tratamiento automatizado de datos personales. La infracción a lo dispuesto en este inciso será sancionada conforme al artículo 23 de la Ley Nº 19.628. Los motores de búsqueda se ajustarán para evitar la búsqueda de causas sobre la base de nombres, rol único tributario u otros datos personales". Sin embargo, esta redacción no prosperó.

Al momento de discutir la norma se tuvo en cuenta que el artículo 9º del COT dispone que "los actos de los tribunales son públicos, salvo las excepciones expresamente establecidas por la ley", tal como sucede con los juicios de familia y estado civil, por mencionar algunos en los cuales la protección de la vida privada es el argumento basal para declarar su reserva.

Ahora bien, es importante considerar que el principio de publicidad de las actuaciones judiciales se establece principalmente en favor de las partes interesadas en el juicio, como uno de los pilares del derecho a defensa, sin embargo en el caso que nos ocupa el legislador optó por la máxima publicidad.

Si bien es cierto que es información verídica la identidad de las partes, la acción que se impetra y los datos referentes a los estadios procesales, respecto del asunto debatido no gozará del sello de veracidad mientras el juicio se encuentre pendiente y será recién la sentencia firme quien determinará la verdad procesal.

Desde el punto de vista de la teoría de la protección de datos, esta solución no parece del todo acertada por cuanto los datos judiciales, en parte importante, no responden al principio de calidad desde el punto de vista de la protección de datos. Nos explicamos: si bien es cierto que es información verídica la identidad de las partes, la acción que se impetra y los datos referentes a los estadios procesales, respecto del asunto debatido no gozará del sello de veracidad mientras el juicio se encuentre pendiente y será recién la sentencia firme quien determinará la verdad procesal.

Otro tema relevante dice relación con la aplicación del artículo 21 de la Ley Nº 19.628, de protección de datos personales, cuando dispone que "los organismos que sometan a tratamiento datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias, no podrán comunicarlos una vez prescrita la acción penal o administrativa, o cumplida o prescrita la sanción o la pena".

Respecto de este artículo, la Corte de Apelaciones de Santiago en autos rol Nº 13.562-2015, en sentencia de 1 de marzo de 2016, consideró que "el artículo 21 de la ley 19.628 debe interpretarse de una forma armónica con el principio general de publicidad de los actos administrativos, y que dicha interpretación exige ajustar su alcance al de una prohibición para organismos públicos que hacen tratamiento de datos para revelar aquellos caducos como sanciones prescritas o cumplidas en las publicaciones o registros confeccionados a partir de determinados datos, pero no puede extenderse a las sanciones contenidas en actos administrativos que originalmente impusieron la medida disciplinaria. Es como si por ejemplo extrapolada la situación al caso de las sanciones penales, se pretendiera que por no poder figurar ya una sanción en el extracto de filiación y antecedentes. Pasare por ello a estar prohibido otorgar copia de la sentencia que la impuso" (ratificada por la CS en queja rol Nº 16.628-2016, desechada).

3.4 Las políticas judiciales en materia de protección de datos personales

La entrada en vigor de la Ley Nº 20.886, sobre tramitación electrónica de juicios civiles, ha reimpulsado la informatización del Poder Judicial. Esta ley debió complementarse con algunos autos acordados de la Corte Suprema y uno de los temas que se debatió en el proceso legislativo dice relación con el tratamiento de datos personales en el marco de la implementación de esta ley, sobre todo porque en su texto se declara como uno de los principios rectores de la nueva forma de tramitar los juicios civiles la publicidad, en los términos que establece el artículo 2 letra c:

> "Los actos de los tribunales son públicos y, en consecuencia, los sistemas informáticos que se utilicen para el registro de los procedimientos judiciales deberán garantizar el pleno acceso de todas las personas a la carpeta electrónica en condiciones de igualdad, salvo las excepciones establecidas por la ley".

Esta norma debía ser compatibilizada con las necesidades de resguardo de los datos personales, especialmente tratándose de datos sensibles. Al respecto, el mismo artículo 2º, en su inciso tercero prevé que "se prohíbe el tratamiento masivo de los datos personales contenidos en el sistema de tramitación electrónica del Poder Judicial, sin su autorización previa. La infracción cometida por entes públicos y privados a lo dispuesto en este inciso será sancionada conforme a la Ley Nº 19.628".

A renglón seguido, se entrega a la Corte Suprema la labor de regular a través de auto acordado la búsqueda de causas en el sistema de tramitación electrónica del Poder Judicial. En virtud de esta delegación del legislador, el auto acordado S/N, Acta Nº 85-2019, de 5 de junio de 2019, establece que se excepciona del acceso libre a las causas y trámites que la ley o por decisión judicial sean reservadas, caso en el cual solo podrán acceder las personas habilitadas.

Adicionalmente, en el auto acordado Acta Nº 71-2016, que regula el funcionamiento de tribunales que tramitan electrónicamente, en su artículo 23 se refiere a la seguridad de los sistemas informáticos en los siguientes términos:

> "Todos los sistemas informáticos deberán proporcionar control en el acceso a la información y seguridad, quedando a cargo de la Corporación Administrativa del Poder Judicial velar por el diseño que un sistema informático que asegure tales objetivos".

Luego, en lo relativo a asegurar la limitación de acceso a las causas o actuaciones sujetas a reserva, el artículo 34 del mismo auto acordado prevé, en su inciso segundo, lo siguiente:

> "Para el caso en que se decrete la reserva de ciertos antecedentes, el tribunal o la unidad que corresponda deberán tomar todas las providencias necesarias para garantizarla, tales como requerir la acreditación de identidad del interviniente en la causa".

Respecto de las causas y actuaciones en que rija el principio de publicidad, en lo que nos interesa, se prevé la posibilidad de buscar causas a partir del nombre de la persona, caso en el cual además deberá combinarse este criterio con la especificación de un tribunal determinado.

La base de datos de causas del Poder Judicial, contenida en poderjudicial.cl, ha sido criticada porque a través del nombre y RUN de la persona se puede buscar información de causas vigentes e históricas, pudiendo extraerse la información relativa a las causas en que aparezcan asociadas las personas titulares de dichos datos, con toda la información personal que haya expuesto dicha persona en sus escritos y en la relación de los hechos objeto del juicio, sin que en ningún momento se recabe su consentimiento.

Sin perjuicio de lo anterior, a nuestro juicio, los titulares de los bancos de datos involucrados no quedarían exentos del deber de información ni de los derechos que emanan para el titular de los datos personales, al menos en lo que respecta al derecho de acceso. A nuestro juicio, la mención de la Ley Nº 20.886 a la ley de protección de datos personales no es suficiente garantía en orden a perseguir la

responsabilidad de quienes pudieren infringir la prohibición, dada la precariedad del régimen infraccional de la Ley Nº 19.628, como podemos apreciar en su artículo 23.

Como paliativo, los términos y condiciones del sitio web del Poder Judicial, que las personas deben aceptar para hacerse usuarios, contemplan que la persona se compromete a utilizar el sistema de forma diligente, correcta y lícita, y a no utilizar la información con propósitos comerciales o para fines que atenten contra los legítimos derechos de terceros, especialmente tratándose de información contenida en causas que mantengan el carácter de reservado, en cualquiera de las competencias.

En todo caso, debemos considerar que el mismo documento contiene también una autorización a todos los usuarios para utilizar la información, imprimirla y almacenarla "para fines personales o académicos, así como generar hipertextos hacia esta página desde sus propios documentos, siempre y cuando se haga sin fines comerciales, manteniendo el usuario la obligación de citar como fuente de su información a www.tramitacionelectronica.cl".[55]

Al respecto, cabe hacer presente que es necesario resguardar de mejor manera el acceso a los datos que constan en las bases de datos del Poder Judicial, puesto que si bien los datos de demandante, demandado, tipo de juicio y antecedentes de hecho que se esgrimen por las partes son efectivos, en el sentido de que constan del proceso, no es menos cierto que muchos de estos datos son controvertidos, por lo que no podemos sostener que cumplan con el principio de calidad del tratamiento de datos, pues mientras no se dicte la sentencia no se podrá sostener que alguna de las versiones de las partes sea la verdadera, al menos desde el punto de vista procesal.

A lo anterior se suma el hecho de que hay personas que usan los accesos al sitio poderjudicial.cl a los solos efectos de investigar posibles clientes a quienes ofrecer servicios legales, o para efectos de verificar si se trata de un trabajador o cliente "conflictivo".

55 Términos y Condiciones - Ley de Tramitación Electrónica - Ley 20.886 - Chile (tramitacionelectronica.cl)

En estas circunstancias, el acceso ilimitado a la base de datos puede prestarse para discriminaciones arbitrarias en contra de las personas, razón de más para reconsiderar las políticas de acceso a esta información.

En esta materia, la Corte Suprema en autos rol Nº 18.818-2019, de 27 de diciembre de 2019, se pronunció respecto de la potencial aptitud del portal de información del Poder Judicial desde la óptica de la protección de datos personales. Sobre el particular, estimó que la "sola existencia del portal en internet del Poder Judicial, que permite acceder a información relevante sobre tramitación y estado de causas, carece de aptitud para lesionar *per se* derechos fundamentales".

Sin perjuicio de lo anterior, estimamos que el Poder Judicial debiera reflexionar sobre los resguardos que cabe adoptar en el portal luego de la reforma constitucional que introdujo la protección de datos como garantía fundamental. Asimismo, de aprobarse el proyecto de ley en actual tramitación en el Congreso Nacional, el Poder Judicial deberá designar un oficial de control de datos personales, quien deberá velar por el adecuado balance entre la obligación de publicidad de las actuaciones judiciales con las necesidades asociadas al resguardo del derecho a la protección de datos personales.

En este mismo ámbito, en sentencia dictada en autos rol Nº 11.626-2019, de fecha 23 de enero de 2020, la tercera sala de la Corte Suprema, conociendo de un recurso de protección interpuesto con motivo de que diversas empresas habrían enviado al domicilio particular del recurrente información sobre la existencia de una demanda ejecutiva en su contra, al respecto señala lo siguiente:

> "(…) y le ofrecen la posibilidad de solución ya sea representándola en juicio o asistiéndola en la negociación extrajudicial del caso, entre otros puntos, acto que considera ilegal y arbitrario atendido el carácter personal de la información contenida en la misiva, cuyo uso, almacenamiento o manipulación nunca autorizó. Asimismo estima que vulnera las garantías constitucionales previstas en los numerales 1, 4 y 24 de la Carta Fundamental, por lo que pide ordenar a la recurrida eliminar de sus bases de datos aquella información personal e incurrir nuevamente en la conducta reprochada, con costas" (Considerando primero).

Al respecto, el Máximo Tribunal estimó que:

> "En este escenario, tal como lo ha resuelto esta Corte con anterioridad, a modo ejemplar en autos CS Rol 12.151-2019, tratándose de antecedentes que se hallan en una fuente de libre acceso al público –y en atención a lo informado por la Corporación Administrativa del Poder Judicial en el sentido que 'debido a que las causas pueden revisarse en la consulta unificada luego de la presentación de la demanda, es posible que la recurrida haya obtenido la información por ese medio'– resulta plausible que hubieran obtenido los datos de una fuente de libre acceso público, esto es, a través de la búsqueda en el portal del Poder Judicial en relación al ingreso de demandas nuevas, como asimismo a través de la publicación del estado diario con el que se notifica a la parte demandante la primera resolución que se dicta en todo procedimiento. Con todo, viene al caso relevar que este hecho no permite por sí solo entender que exista un tratamiento masivo de datos por parte de la entidad recurrida.
>
> Sin perjuicio de lo anterior, la Corporación Administrativa del Poder Judicial deberá adoptar las medidas que sean necesarias para dar estricto cumplimiento a la norma contenida en el inciso 2° de la letra c) del artículo 2° de la Ley N° 20.886, en orden a que las demandas y demás presentaciones que ahí se indican sean accesibles únicamente al solicitante mientras no se haya notificado a su contraparte la resolución recaída en ellas, ello en armonía con lo dispuesto en el artículo 2° inciso 2° del Acta N° 85-2019, de esta Corte, de fecha 5 de junio de 2019, que contiene el 'Texto Refundido del Auto Acordado para la Aplicación en el Poder Judicial de la Ley N° 20.886', que dispone que 'La obligación de reserva que recae sobre las demandas mientras no se haya notificado la resolución recaída en ellas, se entenderá respecto de todo requerimiento que dé origen a un procedimiento judicial'. Ofíciese" (Considerando quinto).

El mismo criterio sigue este tribunal en la sentencia dictada en autos rol Nº 11.627-2019, de 22 de noviembre de 2019, de la tercera sala.

Otro caso relevante, respecto de los datos personales que son objeto de tratamiento con ocasión de la labor de tribunales, es el que dice relación con una solicitud de acceso a la información pública de los nombres, edades y situación penitenciaria de reclusos que cumplían sus condenas en el penal de Punta Peuco. Se trata del fallo recaído en autos rol Nº 26.276-2019, de 26 de febrero de 2020, dictado por la tercera sala en un recurso de queja parcialmente acogido. En este fallo, la Corte Suprema estimó lo siguiente:

> "Dado que esos datos personales se refieren a 'características morales' de los sujetos que se encuentran cumpliendo condena en un centro de cumplimiento penitenciario, salta a la vista que ellos deben ser catalogados como 'datos sensibles', de acuerdo a la letra g) del 2 de la Ley N 19.628, transcrita más arriba" (Considerando 18).
>
> "Que, en esas condiciones, resulta evidente que la publicidad de la información que se solicita en los dos primeros apartados del requerimiento hecho por la señora [*se omite su nombre*], esto es: i.- Nómina de internos que se encuentran condenados en el Centro de Cumplimiento Penitenciario de Punta Peuco al 4 de julio de 2018, incorporando las columnas tarjadas con ocasión de su respuesta, esto es, las denominadas 'interno', 'edad', y 'causa Rol N°'; y ii.- Nómina de los condenados trasladados desde el Centro de Cumplimiento Penitenciario de Punta Peuco a otro Penal; en cuanto incorporan el nombre del interno, corresponde a datos sensibles de los individuos allí incluidos, lo que podría afectar 'los derechos de las personas', constatación de la que se sigue, forzosamente, que en la especie se configura, la causal de reserva prevista en el N° 2 del artículo 21 de la Ley N° 20.285, respecto de los antecedentes solicitados a Gendarmería de Chile por doña... en lo que al nombre de los reclusos se refiere. Así lo ha resuelto esta Corte en casos similares con en el Rol CS N° 19.233-2018.
>
> En efecto, considerando que la información que se ordena entregar, en cuanto se acepta la incorporación de la columna que contempla el nombre de cada interno del penal de Punta Peuco, ha debido ser categorizado como 'datos sensibles', al tenor de

> lo prescrito en el artículo 2 de la Ley N° 19.628, por lo que es evidente que en la especie se ha configurado, la causal de reserva o secreto estatuida en el N° 2 del artículo 21 de la Ley N° 20.285 y que, en consecuencia, no se ha podido hacer lugar a la petición de acceso formulada por doña [*se omite el nombre*] en cuanto al nombre de los internos que cumplen condena en el aludido centro penitenciario y los que han sido trasladados desde allí a otro penal del país. Empero, las recurridas, quebrantando el mandato contenido en la normativa citada, desestimaron la reclamación destinada a denegar el conocimiento, precisamente, de los datos referidos" (Considerando 20).

Otro fallo relevante en materias asociadas al tratamiento de datos personales en el ámbito de la justicia es el recaído en autos rol N° 38690-2019, de 10 de junio de 2020, en que la tercera sala de la Corte Suprema, en apelación de recurso de protección, se pronuncia respecto de la negativa del Servicio Nacional de Registro Civil a borrar antecedentes prontuariales del recurrente.

Al respecto, la Corte señala que la omisión de antecedentes penales "no conlleva la destrucción permanente de las anotaciones prontuariales o del prontuario sino que opera al momento de solicitar el interesado un certificado de antecedentes penales, y permite que el documento no contenga una o más anotaciones prontuariales, las que seguirán existiendo en el prontuario penal. Por su parte, la eliminación de antecedentes no es definida en el Decreto Supremo N° 64, sino que en el artículo 2 letra h) de la Ley N° 19.628 sobre Protección de la Vida Privada de las Personas, como 'la destrucción de los datos almacenados en registros o bancos de datos, cualquiera fuere el procedimiento empleado para ello'. En este sentido, ya sea que la eliminación se refiera a una anotación judicial o a la destrucción íntegra del prontuario, es patente que la acción de eliminar o destruir tiene efectos permanentes en los antecedentes de la persona, puesto que ellos desaparecen. Es preciso subrayar que el D.S. N° 64 emplea indistintamente los términos 'destruir', 'eliminar' o 'borrar', por lo que debe entenderse que su significado y efectos son equivalentes".

Luego, la Corte sigue razonando lo siguiente:

> "Que la 'eliminación definitiva de los antecedentes prontuariales' establecida en el inciso tercero del artículo 38 de la Ley N° 18.216, al ser especial y autónoma respecto de la reglamentación contenida en el D.L. N° 409 y en el D.S. N° 64, no lleva consigo, necesariamente, la destrucción del prontuario, por lo que la regla contenida en el inciso final del mismo precepto legal sigue teniendo plena aplicación para los casos allí consignados.
>
> La 'destrucción' material y definitiva del prontuario en los casos a que se refiere el artículo 38 de la Ley N° 18.216, continúa rigiéndose por los artículos 9 y 10 del D.S. N° 64 de 1960, pero el Servicio de Registro Civil e Identificación está obligado a dar cumplimiento a la orden de eliminación de antecedentes penales que los tribunales con competencia penal le impartan, conforme a la primera de las normas citadas" (Considerando 9º).

3.5 Acción de *habeas data* y su aplicación práctica en Chile

La ley de protección de datos estableció, como mecanismo de tutela efectiva, la acción de *habeas data*, la cual se basó en el recurso de protección, pero fue radicada en los tribunales civiles. El objeto de la acción es la obtención del derecho de acceso, rectificación, eliminación (supresión o cancelación).

Si miramos la experiencia internacional, se distingue entre un *habeas data* "administrativa", que consiste en la solicitud formulada directamente al responsable del fichero (registro o banco de datos) y una etapa judicial, en que se entablan las acciones judiciales frente al silencio, la negativa o la respuesta insuficiente del responsable.

El *habeas data* "administrativo" emana directamente del artículo 12 de la Ley Nº 19.628, en cuyo inciso primero se prevé el **derecho de acceso**, que comprende el derecho de la persona a exigir "a quien sea responsable de un banco, que se dedique en forma pública o privada al tratamiento de datos personales, información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente".

Este derecho incluye la posibilidad del titular de solicitar personalmente y obtener una copia gratuita de los datos de la persona que consten en el registro o banco de datos, en la medida que hayan transcurrido a lo menos seis meses desde la última solicitud.

Luego, el inciso segundo considera el **derecho de rectificación**, para el caso en que los datos personales sean erróneos, inexactos, equívocos o incompletos, y así se acredite. En este caso, además, deberá entregarse a la persona copia del registro modificado.

La **supresión de datos** o **eliminación**, en tanto, se consagra en el inciso tercero, previéndose que procederá en las siguientes hipótesis:

- Si el almacenamiento de datos carece de fundamento legal.

- Si los datos personales devienen en caducos.
- En aquellos casos en que la persona haya proporcionado los datos voluntariamente.
- Cuando los datos ellos se usen para comunicaciones comerciales y la persona no desee continuar figurando en el registro respectivo, sea de modo definitivo o temporal.

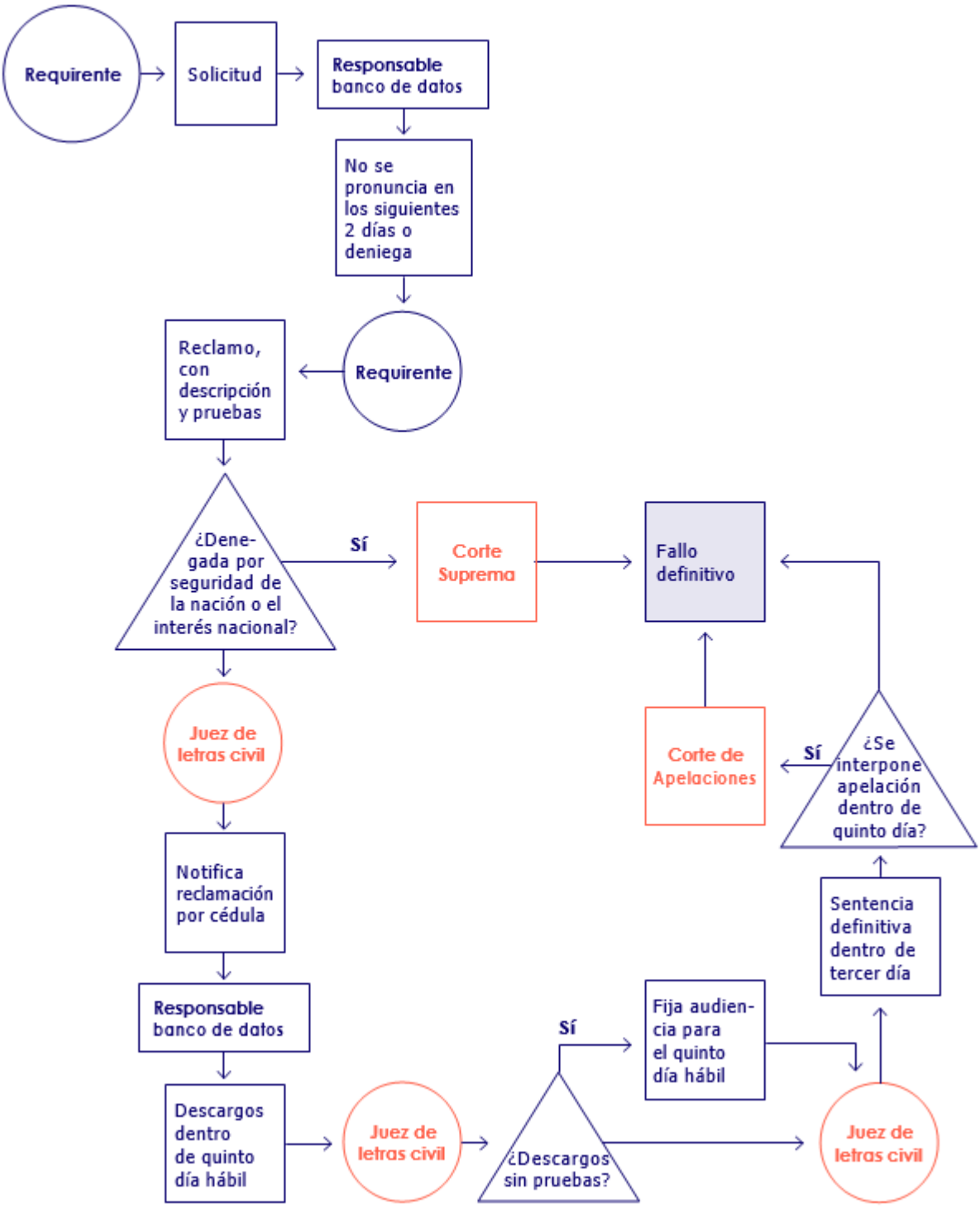
En todo caso, el responsable del registro o banco de datos no podrá exigir un cobro para llevar a cabo el acceso, modificación, eliminación, lo cual se entiende porque es obligación del responsable el tener información de calidad y obtener los datos cumpliendo el principio de licitud. Al respecto, la Corte Suprema, en autos rol Nº 38.666-2017, de fecha 3 de enero de 2018, acogió recurso de protección interpuesto contra Dicom (Equifax Chile S.A.) por la negativa a entregarle al recurrente, sin costo, un registro de sus datos financieros, en circunstancias de que era la primera solicitud que realizaba en el año.

El fallo señala que el derecho previsto en el artículo 12 de la Ley Nº 19.628 es por su naturaleza "personalísimo" reconocido respecto del "titular de los datos almacenados para solicitar un registro actualizado de éstos siempre que haya transcurrido a lo menos seis meses desde la anterior solicitud".

Ahora bien, aun cuando se trata de un derecho que no podrá ser limitado por medio de ningún acto o convención (art. 13) y sin perjuicio de lo cual, la ley limita su ejercicio en el artículo 15, que dispone:

> "No podrá solicitarse información, modificación, cancelación o bloqueo de datos personales 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.
>
> Tampoco podrá pedirse la modificación, cancelación o bloqueo de datos personales almacenados por mandato legal, fuera de los casos contemplados en la ley respectiva".

En sede judicial, la tramitación de esta acción se encuentra regulada en el artículo 16 de la Ley Nº 19.628. En el siguiente esquema podemos apreciar su procedimiento:



Como se puede apreciar, el requirente presenta su solicitud al responsable del banco de datos, quien tiene 2 días hábiles para responder a la solicitud (ejercicio de derechos de acceso, rectificación, cancelación, bloqueo, oposición). Si el titular del registro o banco de datos no responde en ese plazo, la respuesta resulta insatisfactoria o si deniega la solicitud, la persona podrá entablar el *habeas data*.

Para saber cuál es el tribunal competente para ello, habrá de analizarse si la causal de denegatoria fue por razones de seguridad de la nación, de interés nacional u otra causa.

En caso que la causal de denegatoria no fuera una de las señaladas, el tribunal será el juzgado de letras en lo civil del domicilio del responsable del banco de datos, que se encuentre de turno según las reglas correspondientes, solicitando el amparo de estos derechos. Se ha criticado esta regla por cuanto agrega una carga al demandante, al exigirle que se dirija al tribunal del domicilio del demandado, en circunstancias de que resultaría más apropiado, desde la óptica de garantizar la tutela efectiva, que la persona pudiera elegir si dirigirse al tribunal de su domicilio o al del demandado.

En este caso, el procedimiento será el siguiente:

a) Relación de los hechos, la infracción cometida y acompañamiento de los medios de prueba que los acrediten en su caso. Esta exigencia se ha criticado por las dificultades que entraña que el afectado por el tratamiento de datos personales cuente con los medios de prueba que le permitan acreditar los hechos en que se basa la infracción que se imputa al responsable del banco de datos, sobre todo si consideramos que en muchos casos se trata de datos, programas y sistemas que se encuentran en poder del demandado. Ello, máxime si se considera las facilidades que se otorgan al demandado como podemos apreciar a continuación.

b) Notificación al responsable del registro o banco de datos. Luego, el tribunal dispondrá que se notifique por cédula al responsable del banco de datos correspondiente, quien deberá presentar sus descargos dentro de quinto día hábil.

c) A diferencia del demandante, al demandado se le reconoce la opción de presentar las pruebas que acreditan los hechos que esgrima en su libelo conjuntamente con este, o alegar que no dispone de ellos y, en ese caso, el tribunal fijará una audiencia para dentro del quinto día hábil a fin de recibir la prueba ofrecida y no acompañada.

d) La sentencia definitiva deberá dictarse dentro de tercero día desde que haya vencido el plazo para oponer descargos, en caso de que el demandado nada diga, o una vez vencido el plazo de prueba, en caso que se haya decretado audiencia de prueba.

e) La sentencia definitiva será apelable en ambos efectos, debiendo interponerse dentro del término de 5 días contados desde la notificación por cédula de la sentencia a la parte que lo entabla, deberá contener los fundamentos de hecho y de derecho en que se apoya y las peticiones concretas que se formulan.

f)) Deducida la apelación, los autos serán elevados de inmediato a la Corte de Apelaciones respectiva, quien conocerá en cuenta, gozando de preferencia y sin esperar la comparecencia de ninguna de las partes.

g) El fallo dictado en apelación no será susceptible del recurso de casación.

Si la causal invocada fuera seguridad de la nación o interés nacional, el tribunal competente será la Corte Suprema y se sujetará al siguiente procedimiento:

a) Recibida la acción, la Corte solicitará informe al recurrido, fijándole un plazo al efecto, transcurrido el cual resolverá en cuenta la controversia.

b) De recibirse prueba se consignará en un cuaderno separado y reservado, que conservará ese carácter aun después de afinada la causa, si por sentencia ejecutoriada se denegare la solicitud del requirente.

c) La Corte Suprema conocerá en sala en primera instancia, pudiendo deducirse apelación ante la Corte de Apelaciones, en la cual asimismo se conocerá en sala.

d) La sala de una u otra instancia podrá ordenar traer los autos en relación, para oír a los abogados de las partes, caso en el cual la causa se agregará extraordinariamente a la tabla respectiva de la sala de que se trate. La audiencia correspondiente tendrá el carácter de reservada.

Adicionalmente, como señalamos antes, la Ley Nº 20.285, de transparencia y acceso a la información pública, previó que el Consejo para la Transparencia deba velar por el cumplimiento de la Ley Nº 19.628 por parte de los órganos de la administración del Estado (art. 33 letra m de la Ley Nº 20.285). En virtud de esta norma, dicho organismo se ha pronunciado a través de lo que denomina "*habeas data* impropio", esto es, requerimientos de acceso a la información pública en que el solicitante pide a un órgano público información que le concierne. Asimismo, por la vía de reclamos de ilegalidad interpuestos respecto de las resoluciones del Consejo, las Cortes de Apelaciones han debido conocer de estas materias cuando son objeto de debate en sede de transparencia.

En todo caso, el *habeas data* ha tenido escasa aplicación en Chile, en parte porque los requisitos que se exigen no son fáciles de cumplir para las personas, y también porque se han preferido otras vías para reclamar el derecho. Es así como una de las más utilizadas por los titulares de datos, para acceder a su información en poder del Estado, es el acceso a la información pública, que como se dijo ha sido llamado "*habeas data* impropio" por el Consejo para la Transparencia, el que luego podrá ser objeto de amparo ante el Consejo y de reclamación respecto de las resoluciones de dicho órgano y de queja respecto de la resolución de la Corte de Apelaciones.

A vía ejemplar, la Corte de Apelaciones, en autos rol Nº 9644-2017, reclamo de ilegalidad contra la decisión del Consejo para la Transparencia, se pronuncia respecto de la solicitud de acceso de un postulante en un concurso público a los antecedentes correspondientes a su evaluación psicolaboral. En este caso, el voto de mayoría estimó

que el Servicio Civil (Alta Dirección Pública) debía entregar copia del referido informe al solicitante, por ser el titular de los datos personales que en el mismo se consignan, no siendo suficiente la entrega de la nota de calificación final del postulante y su calidad de idóneo o no para el cargo, como podemos ver a continuación:

> "Debido a que como mandata el artículo quincuagésimo tercero de la ley [*Nº 19.882*], la selección es un proceso técnico de evaluación de los candidatos, que incluirá entre otros aspectos, la verificación de los requisitos y la evaluación de los factores de mérito y de competencias específicas, y que se 'expresará en un sistema de puntajes'. Así, tal como lo señala el propio órgano en la letra d) del documento denominado 'aspectos relevantes del proceso de evaluación', producto de la etapa de evaluación psicolaboral y referencias laborales se categoriza a los postulantes en 'idóneo/a', idóneo/a con observaciones' o 'no idóneo/a' atendida la calificación resultante. De esta forma, una interpretación como la efectuada por la reclamada implica entender que 'calificación final' y 'resultado de su evaluación' corresponden a la misma información, puesto que conociéndose la calificación final del postulante se conoce su categoría de 'idóneo/a', 'idóneo/a con observaciones' o 'no idóneo/a', lo que tornaría completamente inútil la distinción efectuada porel legislador" (Considerando 10).

Agrega luego que "el solicitante de la información es precisamente el titular de aquellos datos sensibles que constan en el informe psicolaboral. Por ello, al ser el titular de aquellos datos sensibles, quien solicita su entrega, no puede entenderse que respecto de él rija la reserva o secreto, precisamente porque los datos son de su propiedad. Al titular de datos sensibles le asiste el derecho de solicitarlos, y su entrega no puede ser rechazada, tal como lo ha expresado el Consejo para la Transparencia en la decisión de amparo recurrida. Dicho derecho le asiste por cuanto es el solicitante el único titular de aquellos datos y el ente público, solo tiene el derecho al uso de aquella información para los efectos del proceso de selección, más no ha generado para sí derecho alguno sobre ellos, que importen una causal para excusar su entrega al requirente, por cuanto son datos única y exclusivamente

de dominio del solicitante, sensibles para éste y privativos de su persona" (Considerando 11).

Otra vía intentada por las personas es la acción de protección, que se ha visto potenciada desde la reforma constitucional que reconoció como derecho fundamental la protección de datos personales.

3.6 El régimen infraccionalen la Ley Nº 19.268

De acuerdo a la Ley Nº 19.628, el titular del registro o banco de datos deberá indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de los datos, sin perjuicio de proceder a eliminar, modificar o bloquear los datos de acuerdo a lo requerido por el titular de los datos que se sienta afectado por el tratamiento indebido, o en su caso, lo ordenado por el tribunal.[56]

La acción consiguiente podrá interponerse conjuntamente con la reclamación destinada a establecer la infracción, sin perjuicio de lo establecido en el artículo 173 del Código de Procedimiento Civil. En todo caso, las infracciones no contempladas en los artículos 16 y 19, incluida la indemnización de los perjuicios, se sujetarán al procedimiento sumario. El juez tomará todas las providencias que estime convenientes para hacer efectiva la protección de los derechos que esta ley establece. La prueba se apreciará en conciencia por el juez.[57]

El monto de la indemnización será establecido prudencialmente por el juez, considerando las circunstancias del caso y la gravedad de los hechos.[58] En tal sentido, la jurisprudencia ha establecido indemnizaciones del daño moral a los titulares de datos en montos de fluctúan en un mínimo de $5.000.000[59] a $7.000.000[60], con una media de $25.000.000[61] y un máximo de $70.000.000[62] por cada persona afectada.

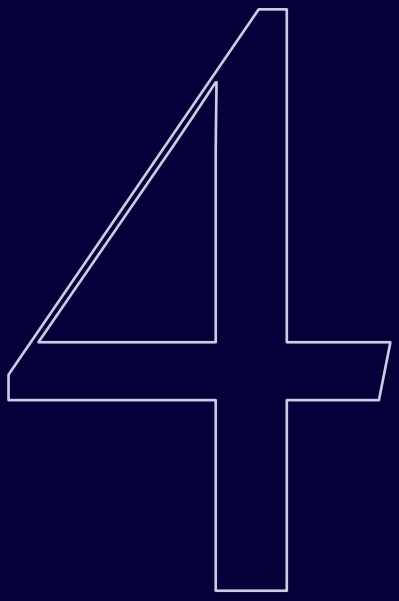
56 Cfr. Ley Nº 19.628, artículo 23.
57 Ídem.
58 Ídem.
59 "A.V.A. con Supermercado Cencosud", rol N° C-22.197-2007, 14° Juzgado Civil de Santiago, confirmado por Ilma. Corte de Apelaciones de Santiago, rol ingreso Corte N° C-6742-2010. Inexistencia de transacción comercial, falta de diligencia o cuidado en la verificación de identidad del tarjetahabiente.
60 "C.U.F. con Corpbanca", Excma. Corte Suprema, 2005. Juicio por negación de crédito hipotecario preaprobado, daño moral causado por violación a la buena fe en la etapa precontractual.
61 Excma. Corte Suprema, rol ingreso N° 3901-2005, autos "L.I.H.B. con CMR Falabella S.A", publicación indebida de un pagaré en base de datos, acoge demanda y resuelve: "Se acoge la demanda de indemnización de perjuicios por $25.000.000.- por concepto de daño moral".
62 "R.S.H. con Corpbanca", Excma. Corte Suprema rol N° 587-2009. Negación de crédito aduciendo deuda inexistente.

Adicionalmente, de acogerse la reclamación en sede de *habeas data*, la sentencia:

- Fijará un plazo prudencial para dar cumplimiento a lo resuelto.
- Podrá aplicar una multa de 1 a 10 Unidades Tributarias Mensuales (UTM), en forma genérica por cualquier infracción a la Ley N° 19.628 y la Ley Nº 20.575.
- Podrá aplicar una multa de 10 a 50 UTM si la infracción es cometida a lo dispuesto en el artículo 17, es decir, sobre datos patrimoniales de naturaleza económico, financiero, bancario o comercial de acceso restringido para el comercio establecido para la finalidad del proceso de crédito y las entidades que participen de la evaluación de riesgo comercial para el fin de evaluación de riesgo comercial; o al artículo 18, es decir, comunicar datos del artículo 17 luego de transcurridos 5 años desde que la obligación se hizo exigible o después de haber sido pagada o haberse extinguido por otro modo legal; sin perjuicio de la comunicación a los tribunales de justicia de la información que requieran con motivos de juicios pendientes (estos artículos se refieren al tratamiento de datos de carácter económico, bancario, financiero y comercial).

El artículo agrega además una infracción por el incumplimiento de lo ordenado por el tribunal, en el inciso final del artículo 16, el cual dispone:

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



Principios y derechos en materia de tratamiento de datos personales. Análisis desde la doctrina y la jurisprudencia.

← Índice de contenidos

4.1 Principio de lealtad y licitud del tratamiento de datos

De acuerdo con la tendencia internacional, en Chile se consideran básicamente dos condiciones de licitud del tratamiento de datos personales: la ley y el consentimiento del titular de los datos personales.

La **lealtad** impone el tratamiento de datos de buena fe, mientras que el principio de **licitud** en realidad constituye una manifestación de la legitimación del tratamiento de datos personales, en tanto manejo de bienes de terceros, respecto de los cuales el responsable del tratamiento debe guardar el deber de custodia. Se manifestará en cada uno de los subprincipios que informan cada una de las fases del tratamiento de datos personales, como supranorma a la que deberá subordinarse tanto la interpretación como su aplicación en el marco de la normativa de protección de datos personales.

A continuación analizaremos cómo se plasman estas reglas en la estructuración de los principios del tratamiento de datos.

4.2 Principio general de legitimación

Conforme al artículo 4º de la Ley Nº 19.628, en Chile se reconocen dos fuentes de legitimación del tratamiento de datos personales: la ley y el consentimiento expreso del titular de los datos, el que además deberá constar por escrito. Luego, el inciso segundo del mismo dispone que "la persona que autoriza debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público".

De acuerdo a este principio, "el tratamiento de los datos personales solo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello".[63] La autorización legal puede provenir de la propia ley N° 19.628 o de otras normas sectoriales de igual o superior rango.[64]

En primer lugar, nos referiremos aquí al consentimiento como legitimante del tratamiento de datos. En esta materia, el principio exige la adopción de medidas necesarias para garantizar que el titular de los datos personales tomó conocimiento general de la existencia de los tratamientos, sus finalidades, responsables y todos aquellos elementos que permitan su correcta identificación y la vigencia de las garantías establecidas en su favor y, por tanto, se encuentre en condiciones de prestar su consentimiento libre e informado.

4.2.1 El consentimiento del interesado

El consentimiento es la manifestación de voluntad acompañada del conocimiento efectivo de las particularidades específicas del tratamiento, incluyendo qué datos que le conciernen serán tratados, cuáles son los mecanismos de recogida, para qué se usarán, a quién o quiénes se comunicarán, cuánto tiempo se mantendrán en el sistema, etcétera.

63 Cfr. Ley Nº 19.629, artículo 4º.
64 Cfr. Declaración Universal de los Derechos Humanos (artículo 12); Pacto Internacional de Derechos Civiles y Políticos (artículo 17); Convención Americana sobre Derechos Humanos (artículo 11).

Como regla general, nuestra legislación exige el consentimiento expreso y tratándose de datos sensibles, además, agrega que debe constar por escrito. La normativa reconoce de esta manera la autonomía de la voluntad del sujeto, permitiendo el tratamiento incluso de datos especialmente protegidos o sensibles.

Como regla general, nuestra legislación exige el consentimiento expreso y tratándose de datos sensibles, además, agrega que debe constar por escrito. La normativa reconoce de esta manera la autonomía de la voluntad del sujeto, permitiendo el tratamiento incluso de datos especialmente protegidos o sensibles.

En aquellos casos en que la ley no exima al responsable del deber de obtener el consentimiento, se requerirá además que la declaración de voluntad del afectado se haga constar de alguna manera que pueda luego ser acreditada.

En efecto, el consentimiento del afectado deberá ser expreso y constar por escrito. La persona que consiente podrá revocar por escrito su autorización para el tratamiento de sus datos, lo cual regirá para lo futuro y sin efecto retroactivo. En el proyecto de ley que se tramita en el Congreso, se prevé una nueva modalidad de consentimiento, que se denomina "inequívoco" y es aquel "que no admite duda o equivocación, que no es susceptible de interpretarse en varios sentidos"; o bien "toda manifestación de voluntad libre, específica, informada y explícita, mediante la que el interesado consiente en el tratamiento de datos personales que le conciernen".[65]

En sede laboral, la Dirección del Trabajo se ha pronunciado respecto de los requisitos del consentimiento a través de ORD. Nº 5589, de 4 de diciembre de 2019, con ocasión del análisis de un documento denominado "Acuerdo de uso de imagen y voz para fines internos", a través del cual una empresa pretendía pactar con sus trabajadores, que se desempeñan como visitadores médicos, para obtener su autorización para el tratamiento de sus datos personales.

La cláusula en comento señala: "De conformidad con la legislación local de Protección de Datos Personales de mi residencia, autorizo a XXX a llevar a cabo el flujo transfronterizo de mis datos personales,

65 Diccionario panhispánico del español jurídico: ver en línea [consulta: 4.02.2021].

incluyendo mi imagen, voz, mi nombre, email, imagen y voz…". Es del caso que la Dirección consideró que esta cláusula no cumple los requisitos legales por las siguientes razones:

— "los términos de la solicitud carecen de la precisión necesaria para asegurar el correcto tratamiento de los datos personales de los trabajadores";

— "el término 'terceros', para referirse a sus filiales, resulta poco preciso y podría prestarse para la externalización de la información", y

— "la enumeración pareciera ser solo ejemplificadora, pero no excluiría el tratamiento de cualquier otro antecedente que posea la compañía respecto de sus trabajadores".

4.2.2 La autorización legal como legitimante

La obligación de recabar el consentimiento no es absoluta, pues la ley prevé hipótesis en las cuales no se requiere el consentimiento del afectado[66], a saber:

a. El tratamiento de datos personales que **provengan o se recolecten de fuentes accesibles al público**, cuando sean de carácter económico, financiero, bancario o comercial, en cuyo caso la autorización de tratamiento se construye a través de la Ley Nº 19.628 y Nº 20.575, además de la Ley Nº 18.010 sobre obligaciones de crédito y las normas de la Superintendencia de bancos, respetando las condiciones que señalan dichas leyes.[67]

b. Los datos que se contengan en **listados relativos a una categoría de personas** y 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.

66 Cfr. Ley Nº 19.628, artículo 4º incisos quinto y final.

67 La Ley Nº 20.575, que establece el principio de finalidad en el tratamiento de los datos personales y fue publicada en el Diario Oficial de fecha 17 de febrero de 2012, en su artículo 1º establece que los datos de protestos y morosidades de los documentos y emisores de créditos allí señalados, exclusivamente, pueden ser comunicados para evaluación de riesgo comercial por las entidades que participen en el riesgo comercial y para el proceso de crédito por el comercio establecido. En todos los demás casos, los datos de solvencia patrimonial y crédito del artículo 17 solo podrán ser comunicados con el consentimiento de su titular.

En cada caso concreto, se debe analizar si el tratamiento de datos que se realizará requiere el consentimiento o basta la autorización legal para realizarlo, lo que supone el análisis de la normativa sectorial en concordancia con la normativa de protección de datos personales.

c. Que los datos sean **necesarios para comunicaciones comerciales** de respuesta directa o comercialización o venta directa de bienes o servicios.

d. El tratamiento de datos personales que **realicen personas jurídicas privadas** para el uso exclusivo suyo, de sus asociados y de las entidades a las que están afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquellos.

e. El tratamiento de datos que **realicen organismos públicos** dentro de la órbita de su competencia y con sujeción a las reglas y principios de tratamiento de datos contempladas en la Ley Nº 19.628. En el capítulo relativo al tratamiento de datos por organismos públicos, ahondaremos en esta materia.

En todo caso, el que se exima del consentimiento no implica que no se deba informar adecuadamente del tratamiento de datos, para que una persona pueda ejercer sus derechos.

Es importante considerar que, en cada caso concreto, se debe analizar si el tratamiento de datos que se realizará requiere el consentimiento o basta la autorización legal para realizarlo, lo que supone el análisis de la normativa sectorial en concordancia con la normativa de protección de datos personales.

Veamos un ejemplo.

En materia bancaria, atendida la prohibición establecida en el inciso tercero del N° 4 del artículo 84 de la Ley General de Bancos, se excluye de todo crédito a los directores de banco, o a cualquiera persona que se desempeñe en él como apoderado general. Asimismo, prohíbe todo crédito a las siguientes personas relacionadas con los directores o apoderados por los vínculos que se indican: cónyuge, hijos menores bajo patria potestad y sociedades en las que cualquiera de ellos forme parte o tenga participación.

Al desarrollar esta exclusión, la Circular N° 3.442 (18.08.08) de la Superintendencia da cuenta de una serie de datos personales que podrán ser tratados por los bancos para la finali-

dad consagrada en el artículo mencionado, sin necesidad de recabar el consentimiento informado, expreso y por escrito, del titular de los datos, incluyendo un cliente, titular de un crédito de consumo.

a. Respecto de directores y apoderados:

— Para elaborar **bases de datos de directores**, de un banco, o a cualquiera persona que se desempeñe en él como apoderado general.

— Para elaborar bases de datos de personas relacionadas a los directores o apoderados por los vínculos que se indican: cónyuge, hijos menores bajo patria potestad y sociedades en las que cualquiera de ellos forme parte o tenga participación.

b. Respecto de los solicitantes y titulares de créditosde consumo:

Siendo así, el banco, sin necesidad de contar con el consentimiento informado, expreso y por escrito, del cliente, titular de un crédito de consumo:

— **Contar con bases de datos de directores**, de un banco, o a cualquiera persona que se desempeñe en él como apoderado general.

— Hacer tratamiento de datos de personas relacionadas a los directores o apoderados por los vínculos que se indican: cónyuge, hijos menores bajo patria potestad y sociedades en las que cualquiera de ellos forme parte o tenga participación.

— Utilizar los datos personales recabados de sus clientes en la solicitud de crédito de consumo.

— Informar a la Superintendencia de bancos sobre los créditos de consumo del titular de datos y sus estados de pago.

— Consultar a los distribuidores de información económica, bancaria, financiera o comercial los datos sobre morosidades de la persona para la evaluación de riesgo comercial.

— Informar a los distribuidores de datos de información económica, bancaria, financiera o comercial, los datos sobre morosidades de la persona.

— Transferir los datos que sean necesarios a las compañías de seguros, para la evaluación de riesgo asociada a las pólizas de seguro relacionadas a los créditos de consumo en evaluación y/o pactados con el banco.

— Tratar los datos personales de los socios de las sociedades, por cuanto es de la naturaleza y finalidad el análisis de solvencia patrimonial para predecir la capacidad de pago de los socios.

En el último caso, no obstante que la sociedad forma una persona jurídica distinta de los socios individualmente considerados[68], la insolvencia de la sociedad de personas, sean civiles o comerciales, obliga el patrimonio y solvencia de sus socios. Así, en la sociedad de personas civiles, la insolvencia de la sociedad se divide entre los socios a prorrata de su interés social, y la cuota del socio insolvente gravará a los otros[69]; en el caso de las sociedades de personas colectivas comerciales, los socios son responsables solidariamente[70] de

68 Inciso final del artículo 2053 del Código Civil.
69 Inciso primero del artículo 2095 del Código Civil.
70 Artículo 1511 inciso segundo del Código Civil: "Pero en virtud de la convención, del testamento o de la ley puede exigirse a cada uno de los deudores o por cada uno de los acreedores el total de la deuda, y entonces la obligación es solidaria o *insólidum*".

todas las obligaciones legalmente contraídas bajo la razón social, en ningún caso podrán derogarla[71], y, en las sociedades de personas, sean civiles o comerciales, cuya responsabilidad personal de los socios se haya limitada a sus aportes o a la suma que a más estos indiquen o solidaria, en el evento de la omisión de los requisitos de constitución o en la falta de la palabra "limitada".[72]

Sin embargo, en las sociedades de capital, tales como las sociedades anónimas[73], en comandita por acciones, y las sociedades por acción, su esencia es su patrimonio y la limitación de la responsabilidad de los accionistas al monto representado en el título negociable, que puede ser transferido libremente, por lo que "hasta el nombre del accionista es irrelevante en el mercado"[74], ni aun las personas naturales que integran el directorio son relevantes, ya que estos son esencialmente revocables.

Como podemos apreciar, en cada materia se puede realizar este mismo árbol de decisión al momento de determinar las condiciones de licitud del tratamiento de datos personales, ya sea en el ámbito de la salud, de la educación, del consumo, y un largo etcétera. De eso hablamos cuando señalamos que la ley de protección de datos personales es una norma de carácter general y supletorio, cuya aplicación deberá analizarse en cada área concreta.

4.2.3 El interés legítimo como "legitimante"

Las legislaciones reconocen situaciones en las cuales será legítimo el tratamiento de datos personales, sin que medie el consentimiento del afectado. Si bien podríamos haber tratado este punto en el acápite de autorización legal como legitimante, estimamos que es más apropiado diferenciar su análisis para una mejor comprensión.

71 Incisos primero y segundo del artículo 370 del Código de Comercio.
72 Artículos 2º, 3º y 4º de la Ley N° 3.918 sobre sociedades de responsabilidad limitada.
73 El artículo 1º inciso primero de la Ley Nº 18.046, señala: "La sociedad anónima es una persona jurídica formada por la reunión de un fondo común, suministrado por accionistas responsables sólo por sus respectivos aportes y administrada por un directorio integrado por miembros esencialmente revocables".
74 PUGA VIAL, Juan Esteban: *La sociedad anónima y otras sociedades por acciones en el derecho chileno y comparado*. Editorial Jurídica, edición 2011; p. 69.

La primera causal que se reconoce como interés legítimo se caracteriza como un "interés público importante". Este interés podría ser el interés de la nación, caso en el cual estaremos ante razones de interés general de la comunidad, que hacen necesario el tratamiento de datos personales. A vía ejemplar, en pandemia, es necesario resguardar la salud de la población, por lo cual la legislación sanitaria prevé la posibilidad de tratar datos personales que sean necesarios para impedir o al menos mitigar los efectos de la propagación del virus.

En este caso, se estima que el interés general prima sobre la intimidad, razón por la cual se autoriza el tratamiento. Sin embargo y atendida la calidad de garantía individual de la protección de datos, en cada caso se deben prever las condiciones o requisitos para que el tratamiento de datos no se traduzca en intromisiones ilegítimas en las esferas protegidas de la persona. Entre las reglas, destacan aquellas relativas a la exigencia de que el tratamiento de datos sea realizado por un profesional sanitario, sujeto al secreto profesional, en virtud de la legislación nacional, o de las normas establecidas por las autoridades nacionales competentes, o por otra persona sujeta a una obligación equivalente de secreto.

Ahora bien, el problema aquí viene dado por la necesidad de dotar de contenido a la expresión "interés público importante" o "interés de la nación", conceptos indeterminables *a priori*, esencialmente mutables y que, en todo caso, estarán condicionados por la concepción del Estado que impere en un momento y lugar determinado.

Otro caso en que existe un interés legítimo es el tratamiento de datos relativos a infracciones, condenas penales o medidas de seguridad, caso en el cual el tratamiento es necesario para finalidades relativas a la justicia penal y política criminal de un Estado. Para salvaguardar los derechos del afectado e impedir que, en base a estos antecedentes, se puedan tomar decisiones arbitrarias a su respecto o intrusiones ilegítimas, estos datos debieran ser tratados por una autoridad pública, previéndose garantías específicas en el derecho nacional.

Una tercera hipótesis dice relación con los tratamientos de datos necesarios para la realización de una determinada relación jurídica, en la medida que el tratamiento sea necesario para respetar obligaciones y derechos específicos del responsable del tratamiento de datos.

Asimismo, otro caso en que procede es el derecho de asociación; de esta forma se legitima a las asociaciones o cualquier otro organismo sin fin de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, para efectuar tratamiento de datos personales bajo las siguientes condiciones: que sea efectuado en el curso de sus actividades legítimas; que se dispongan las debidas garantías; que se refiera exclusivamente a sus miembros o a las personas que mantengan contactos regulares con la entidad de que se trate en razón de su finalidad, y que los datos no se comuniquen a terceros sin el consentimiento del interesado.

Otra circunstancia es ante necesidad de satisfacer un interés legítimo de la persona responsable del tratamiento, recayendo en el titular del registro o banco de datos justificar dicho interés, por ejemplo, la necesidad de dar cumplimiento a una obligación legal o administrativa impuesta sobre la persona responsable por la legislación nacional aplicable, esto es, llevado a cabo por un órgano de la administración pública que así lo precise para el legítimo ejercicio de sus competencias.

Finalmente, se reconoce este interés cuando concurran situaciones excepcionales que pongan en peligro la vida, la salud o la seguridad del interesado o de otra persona[75], como es el caso de la grabación de las rutinas de conducción de un chofer de locomoción colectiva o la recolección de datos de acceso a áreas restringidas.

Si bien la Ley Nº 19.628 no reconoce expresamente el interés legítimo, siguiendo la tendencia internacional, las hipótesis de tratamiento de datos personales sin requerir consentimiento del afectado, tales como el tratamiento de datos para finalidades de marketing directo, se basan en esta causal. En el proyecto de ley en tramitación se busca incorporar expresamente el interés legítimo.

75 Cfr. Resolución de Madrid; p. 15.

En Europa, el RGPD prevé al respecto, en su artículo 6 letra f, lo siguiente:

> "El tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño".

Como se puede apreciar, en cada caso se deberá hacer una ponderación de los intereses y derechos tanto del responsable del tratamiento como del interesado o afectado por el tratamiento de datos.

El antiguo Grupo de trabajo sobre protección de datos del Artículo 29 emitió un dictamen el año 2014[76], con ocasión de la interpretación y aplicación práctica del artículo 7 de la Directiva 46/95, lo que nos ayuda a comprender los elementos que se deben ponderar en cada caso, a saber:

a. **Finalidad legítima:** "la naturaleza y la fuente del interés legítimo, y si el tratamiento de datos es necesario para el ejercicio de un derecho fundamental, resulta de otro modo de interés público o se beneficia del reconocimiento de la comunidad afectada".

b. **Proporcionalidad:** "la repercusión para el interesado y sus expectativas razonables sobre qué sucederá con sus datos, así como la naturaleza de los datos y la manera en la que sean tramitados".

c. **Tutela efectiva al interesado:** "las garantías adicionales que podrían limitar un impacto indebido sobre el interesado, tales como la minimización de los datos, las tecnologías de protección de la intimidad, el aumento de la transparencia, el derecho general e incondicional de exclusión voluntaria y la portabilidad de los datos".

76 Véase Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE. Disponible en línea [consulta: 02.02.2021].

En la doctrina nacional, Pablo Contreras[77] ha señalado que el ejercicio de ponderación incluirá "la utilidad (beneficio material) que una o varias operaciones específicas de tratamiento de datos personales ajenos reporta al sujeto interesado, entendidas como herramientas idóneas (vínculo directo) para satisfacer una necesidad (interés) tutelado por el derecho, y el grado en que los derechos o la esfera jurídica del titular de datos se ven negativamente afectados por dichos tratamientos (externalidad)".

En cuanto al alcance de la legitimación, se ha estimado que permite no solo el tratamiento de datos que consten en fuentes accesibles al público, sino además podría incluir tratamiento de datos que consten en fuentes no abiertas. Así lo estimó la sentencia TJUE, de 24 de noviembre de 2011[78]:

"El artículo 7, letra f), de la 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, debe interpretarse en el sentido de que se opone a una normativa nacional que, para permitir el tratamiento de datos personales necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, exige, en el caso de que no exista consentimiento del interesado, no solo que se respeten los derechos y libertades fundamentales de éste, sino además que dichos datos figuren en fuentes accesibles al público, excluyendo así de forma categórica y generalizada todo tratamiento de datos que no figuren en tales fuentes".

77 CONTRERAS, Pablo: "Interés legítimo y tratamiento de datos personales: antecedentes comparados y regulación en Chile". En *Revista Chilena de Derecho y Tecnologías*, versión en línea ISSB 0719-2584. Vol. 8 Nº 1, Santiago, junio de 2019.

78 Autos acumulados C–468/10 y C–469/10 (caso ASNEF), disponible en línea [consulta: 02.02.2021].

4.3 Principio de transparencia (información y publicidad)

Este principio encuentra su fundamento legal en los artículos 3º y 4º de la Ley N° 19.628. Para su realización, el responsable deberá contar con **políticas transparentes** en lo que a tratamientos de datos de carácter personal que realice se refiere.[79]

En consecuencia, este principio exige la adopción de las medidas necesarias para garantizar el conocimiento general de la existencia de los tratamientos, sus finalidades o propósitos, los responsables del tratamiento de datos, y todos aquellos elementos que permitan su correcta identificación y la vigencia de las garantías establecidas en favor de los titulares de datos personales.

Tradicionalmente, el deber de transparencia impone las obligaciones de registro de las actividades de tratamiento de datos, para que la ciudadanía en general tome conocimiento de su existencia (aun cuando hoy se está abandonando esta obligación frente a le evidencia del tratamiento de datos generalizado). Adicionalmente, incluyen el deber de información, que es requisito del consentimiento.

4.3.1 Deber de notificación y Registro

A la época de la dictación de nuestra ley, como regla general se preveía el deber de notificación, obligación que recae en el responsable del tratamiento, o en su caso en su representante, de efectuar una comunicación a la autoridad de control con anterioridad a la realización de un tratamiento o de un conjunto de tratamientos de datos personales. Esto, a fin de asegurar la publicidad de los fines del tratamiento y de sus principales características y dar así vigencia a los principios de transparencia o publicidad y al principio de control o tutela efectiva a los interesados.

79 Cfr. Resolución de Madrid; p. 12.

A vía ejemplar, en el caso español se debía notificar a la Agencia de Protección de Datos, en Alemania a la Comisión de Protección de Datos, en Suecia a la Inspección de Datos y, en Francia, a la Comisión Nacional de Informática y Libertades.

Si bien en Chile no se previó en la ley una autoridad de control del tratamiento de datos, se consideró que este deber se restringía a los organismos públicos. Y el organismo al cual estos notifican sus tratamientos de datos es el Servicio Nacional de Registro Civil, que mantiene un sitio web en el cual las distintas reparticiones públicas comunican la creación o modificación de los registros o bancos de datos que mantienen.[80]

4.3.2 Deber de información

El deber de información está íntimamente relacionado con obtener el consentimiento del interesado. En este contexto, el principio de información exige que poner en conocimiento del titular de los datos solicitados todos los antecedentes necesarios acerca de las circunstancias y fundamentos del tratamiento, así como de su derecho a prestar o no consentimiento y las consecuencias de su decisión.

En aquellos casos en que los datos de carácter personal hayan sido obtenidos directamente del interesado, la información deberá ser facilitada en el momento de la recogida, salvo que se hubiera facilitado con anterioridad. La información incluirá, al menos: la identidad del responsable del tratamiento y, en su caso, de su representante; los fines del tratamiento de que van a ser objeto los datos, y cualquier otra información que sea necesaria para el adecuado resguardo de sus derechos, tales como los destinatarios o categorías de destinatarios de los datos, el carácter obligatorio o no de la respuesta y las consecuencias que tendría una negativa a responder.

Si los datos de carácter personal no han sido obtenidos directamente del interesado, la información deberá ser facilitada en un plazo prudencial de tiempo[81], si bien podrá sustituirse por medidas

80 El registro se puede consultar en Banco de datos personales (registrocivil.cl) [consulta: 11.02.2021].
81 Habrá que determinar en cada caso concreto que se entiende por plazo prudencial, a estos efectos.

alternativas cuando su cumplimiento resulte imposible o exija un esfuerzo desproporcionado.[82] Como regla general, en este caso los estándares internacionales exigen que se informe al afectado desde el momento mismo del registro de los datos o, en caso de que se piense comunicar datos a un tercero, a más tardar en el momento de la primera comunicación. La información a incluir es la siguiente:

- la **identidad del responsable** del tratamiento y, en su caso, de su representante;
- la **finalidad del tratamiento de datos** y cualquier otra información, como la categoría de los datos de que se trate, los destinatarios o las categorías de destinatarios de los datos, la existencia de derechos de acceso y rectificación de los datos que la conciernen, en la medida que, habida cuenta de las circunstancias específicas en que se hayan obtenido los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado.

Si los datos de carácter personal son recogidos en línea, a través de redes de comunicaciones electrónicas, el deber de información podrá satisfacerse mediante la publicación de políticas de privacidad fácilmente accesibles e identificables,

Si los datos de carácter personal son recogidos en línea, a través de redes de comunicaciones electrónicas, el deber de información podrá satisfacerse mediante la publicación de políticas de privacidad fácilmente accesibles e identificables, que incluyan todos los extremos anteriormente previstos.[83]

En todo caso, cualquier información que se proporcione al interesado deberá facilitarse de forma inteligible, empleando para ello un lenguaje claro y sencillo, en especial en aquellos tratamientos dirigidos específicamente a menores de edad.[84]

Se busca que las personas tengan la posibilidad de tomar conocimiento de los datos de identificación de la persona natural o jurídica que realiza el tratamiento de datos, los datos específicos que son objeto de tratamiento y el peso específico que se asigna a cada uno de los

82 Ídem.
83 Ídem.
84 A estos efectos, debiera considerarse el lenguaje adecuado para el lector promedio de cada grupo objetivo al cual se dirige la comunicación.

datos en el resultado final, esto es, la finalidad del registro, además de la mantención del registro y entrega de antecedentes respecto de quienes han consultado a una determinada persona.

Veamos un ejemplo.

En materia bancaria, la autoridad sectorial ha detallado las implicancias del principio de información de una manera que resulta útil a efectos de ilustrar sus alcances.

La Circular N° 3.429 (25.03.2008) de la Superintendencia de bancos fue de las primeras normas que se ocuparon de esta materia, señalando que:

> "Entre las condiciones necesarias para que la entrega de información cumpla con la propiedad de transparencia, se pueden mencionar:
>
> a) Claridad. Una información es clara si permite al público en general comprender su significado. Para ese efecto se debe usar palabras simples y de común entendimiento.
>
> b) Debe ser completa, de manera que abarque todos los precios, condiciones y características relevantes relacionados con la contratación de un producto y/o servicio, de manera que el cliente pueda conocer el valor final de la prestación. No se cumple con esto último si faltan datos que permitan la realización de un cálculo relacionado.
>
> c) Debe ser relevante, esto es, que sea importante y necesaria para comprender el tema de que se trata en su cabal dimensión. Relevante implica especificar todos los aspectos necesarios para la toma de decisiones.
>
> d) Debe ser fiable, es decir, que sea una representación fiel de la realidad, que no contenga errores, ni que lleve a confusión o duda respecto de su veracidad.

> e) Debe ser comparable, de forma de poder cotejar productos similares ofrecidos por el mismo banco u otros. No será comparable si la forma en que la información se presenta impide o dificulta en forma importante la confrontación con otras opciones.
>
> Esta Superintendencia considera altamente conveniente que cada empresa tenga disponible un plan básico del respectivo producto con su correspondiente precio, a fin de permitir a los clientes su comparación con los similares que ofrezca la competencia.
>
> f)) Debe ser oportuna en el sentido de estar presente en el momento de la toma de decisiones, es decir, que el cliente pueda conocer todas las condiciones con la debida antelación para celebrar un contrato.
>
> g) Debe ser de fácil acceso y gratuita a través de distintos medios tales como folletería y pizarras".

Tal y como sucede en el caso del principio de legitimación, el deber de información tiene excepciones. En primer lugar, este derecho no será aplicable a la recogida de datos cuando la información al afectado impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las administraciones públicas o cuando afecte a la defensa nacional o a la seguridad pública o a la persecución de infracciones penales o administrativas.

Asimismo, no será necesaria la información, si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

En la experiencia comparada, destaca en esta materia la guía para el cumplimiento del deber de informar de las autoridades españolas de protección de datos personales.[85]

85 Véase la Guía para el cumplimiento del deber de informar, de la Agencia Española de Protección de Datos. Disponible en línea [consulta: 04.02.2021].

4.4 Principio de finalidad

El principio de finalidad exige que los datos personales que no provengan de fuentes accesibles al público deben utilizarse solo para los fines para los cuales hubieren sido recolectados.

El artículo 9º de la Ley Nº 19.628 sienta las bases de este principio, cuando dispone que "los datos personales deben utilizarse solo para los fines para los cuales hubieren sido recolectados" si es que el dato no proviene de una fuente de acceso público. En todo caso, la finalidad debe ser legítima e informada y además, en algunos casos, deberá ser consentida por el titular de los datos tal y como sucede en el caso de los datos sensibles y de datos económicos, bancarios financieros y comerciales. Tratándose de organismos públicos, la finalidad estará además determinada por las competencias del responsable del tratamiento.

Como efecto de este principio, el responsable se abstendrá de llevar a cabo tratamientos de datos no compatibles con las finalidades para las que se recolectaron los datos de carácter personal, a menos que cuente con el consentimiento inequívoco del interesado.[86] Así por ejemplo, un banco solo podrá tratar los datos personales de sus clientes, fiadores o deudores solidarios que digan relación con los requisitos necesarios para el cumplimiento de los contratos que mantengan con ellos.[87]

Complementariamente, el artículo 1º de la Ley Nº 20.575 dispone que respecto del tratamiento de datos personales de carácter económico, financiero, bancario o comercial a que se refiere el Título III de la Ley Nº 19.628, sobre protección de la vida privada, "deberá respetarse el principio de finalidad en el tratamiento de datos perso- nales, el que será exclusivamente la evaluación de riesgo comercial y para el proceso de crédito", y por ende la comunicación de esta

86 Cfr. Resolución de Madrid; p. 10
87 Entendemos que estos pueden ser de su esencia, de su naturaleza o meramente accidentales.

clase de datos "solo podrá efectuarse al comercio establecido, para el proceso de crédito, y a las entidades que participen de la evaluación de riesgo comercial y para ese solo fin".

Entendemos que estamos ante normas "imperativas de requisitos", que fijan las condiciones de legitimidad del tratamiento de datos personales.

En el caso del RGPD europeo, como regla general establece que "los datos personales serán recogidos con fines determinados, explícitos y legítimos y no serán tratados ulteriormente de manera incompatible con dichos fines". A partir de ello se habla de "limitación de la finalidad".

4.5 Principio de calidad

El principio de calidad del tratamiento de datos personales constituye el paraguas bajo el cual se engloban las consecuencias de un tratamiento de datos idóneo, tanto desde la óptica de la calidad de los procesos y sistemas empleados en el tratamiento de datos como de los datos en sí mismos.

Adicionalmente, se reconoce como "de calidad" un tratamiento de datos que cumple con los requisitos de legitimidad y licitud. Su origen se remonta al Proyecto Baker (1969) y por ende a los inicios de la doctrina sobre la configuración y alcances doctrinarios de la *Privacy* en el entorno anglosajón.

En su momento, la Directiva Europea 46/95, en su artículo 6, se refirió a este principio. Actualmente, el RGPD a través de sus normas y principios trata exhaustivamente las condiciones de un tratamiento de datos de calidad. En efecto, la calidad de datos impone deberes ligados a la idoneidad de la información seleccionada y la legitimidad/legalidad de su tratamiento en este tipo de procesos, la adecuación de los algoritmos, la publicidad del tratamiento de datos personales y la temporalidad del tratamiento de los datos personales, entre otros factores relevantes, como se verá a continuación.

4.5.1 Condiciones relativas a la calidad de los datos personales

Para que los datos personales sean idóneos, deberán ser adecuados, pertinentes y no excesivos, esto es, limitados a lo necesario en relación a los fines para los cuales son tratados. Al respecto se debe considerar lo dispuesto en el artículo 9º de la Ley Nº 19.628, en tanto exige que "la información debe ser exacta, actualizada y responder con veracidad a la situación real del titular de los datos". ¿Qué implica esto?

- que la información sea **exacta**, es decir "puntual, fiel y cabal";
- que sea **actualizada,** entendiendo por ello "que existe, sucede o se usa en el tiempo de que se habla", y

— que sea **verídica**, lo que supone que se trata de un "juicio o proposición que no se puede negar racionalmente".

Si bien estas cualidades habrán de apreciarse en cada caso concreto, de los conceptos recién transcritos, proporcionados por el Diccionario de la Real Academia Española de la Lengua, se desprende que en la medida que la situación personal del titular de los datos cambie, deberá asimismo modificarse los datos personales contenidos en el registro.

En consecuencia, la veracidad, exactitud quedan condicionadas por la **actualidad**, lo cual conlleva que en todo momento el dato que es objeto de tratamiento debe ir modificándose para adecuarse a la situación de la persona en cada momento.

La mala calidad de los datos personales puede redundar en perjuicios a la persona, en el sentido de que terceros pueden adoptar decisiones adversas a sus intereses o contrarias a sus derechos. Al respecto, la Corte de Apelaciones de Santiago, en sentencia dictada en autos rol Nº 8.304-2014, de fecha 13 de septiembre de 2016, estimó que "la errada comunicación de una morosidad inexistente por parte de la entidad demandada y la posterior publicación de dicha desacertada información en el boletín comercial, impidió al demandado continuar con su postulación a un trabajo que representaba un ascenso laboral en su lugar de empleo, actuación culpable y negligente que, independientemente de que pueda entenderse aliada a otras conductas de terceros ajenos al juicio que contribuyeron a encausar los sucesos en el sentido antes referido, privó al actor de una oportunidad o una chance".

4.5.1.1 Pertinencia de los datos

Que los datos sean pertinentes implica que correspondan al ámbito y finalidad del registro o banco de datos, esto es, que los datos sean adecuados, atingentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente. De lo anterior surgen consecuencias jurídicas de la mayor relevancia, a saber:

a. El deber de **cancelar** aquellos datos que hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados y registrados.

b. La obligación de **anonimizar** o disociar aquellos datos que ya no sea necesario mantener identificados para cumplir la finalidad, esto es, "todo tratamiento de datos personales de manera que la información que se obtenga no pueda asociarse a persona deter-minada o determinable" (art. 2 letra l, Ley Nº 19.628).

c. El deber de **minimización de datos**, esto es, limitar la recogida de datos a lo estrictamente necesario y eficiente para la obtención de la finalidad.

Como podemos apreciar, este principio afecta a todas las etapas del tratamiento de datos personales. Incluso en la fase de creación del registro o banco de datos, exige la predeterminación de las finalidades del tratamiento y los datos personales que serán objeto del mismo.

En cuanto al origen del principio de calidad y pertinencia del tratamiento de datos personales, este se encuentra en el Proyecto Baker, en cuanto sostiene que "la recogida de datos debe guiarse por el principio según el cual se memorizan solo los datos relevantes para la finalidad para la cual se ha creado el banco de datos y según la cual los datos solo son accesibles para estos fines".

4.5.1.2 Exactitud y actualización

Los datos registrados deben reflejar con veracidad la situación real del titular en un momento determinado. De esta manera, infringe el principio todo aquel tratamiento que, de cualquier manera, pueda inducir a un error de apreciación de la situación personal del interesado.

Ya el Convenio Nº 108 reconoció como requisito la exactitud, en su artículo 5 letra d, donde señala que los datos registrados deben ser exactos y, si fuere necesario, tenidos al día y en la letra e de ese mismo artículo, que impone el deber de conservación, en tanto exige que los datos deben ser conservados en forma que permita la identificación de los interesados durante un plazo que no exceda del necesario para los fines para los que fueron registrados. Como consecuencia, el responsable del tratamiento tendrá los siguientes deberes:

a. **Rectificación:** actualización de los datos que sean inexactos o erróneos, ya sea porque nunca fueron exactos o devinieron en incorrectos por cambio en las circunstancias.

b. **Supresión, eliminación o cancelación:** cuando los datos hayan caído en obsolescencia o hayan caducado, procederá "la destrucción de datos almacenados en registros o bancos de datos, cualquiera fuere el procedimiento empleado para ello" (art. 2º letra h, Ley Nº 19.628).

c. **Bloqueo:** "la suspensión temporal de cualquier operación de tratamiento de los datos almacenados" (art. 2º letra b, Ley Nº 19.628) procederá cuando los datos sean de dudosa veracidad o resulte inconveniente su tratamiento, sin que proceda una eliminación.

A vía ejemplar, los artículos 17 y 18 de la Ley Nº 19.628 proscriben la comunicación de datos relativos a algunas morosidades, por las siguientes circunstancias:

— las que **no constan en los documentos autorizados:** "letras de cambio y pagarés protestados; cheques protestados por falta de fondos, por haber sido girados contra cuenta corriente cerrada o por otra causa; como asimismo el incumplimiento de obligaciones derivadas de mutuos hipotecarios y de préstamos o créditos de bancos, sociedades financieras, administradoras de mutuos hipotecarios, cooperativas de ahorros y créditos, organismos públicos y empresas del Estado sometidas a la legislación común, y de sociedades administradoras de créditos otorgados para compras en casas comerciales";

— las que han sido **exceptuadas por el legislador:** deudas por servicios básicos, créditos concedidos por el Instituto Nacional de Desarrollo Agropecuario (Indap) a sus usuarios y la información relacionada con obligaciones de carácter económico, financiero, bancario o comercial en cuanto hayan sido repactadas, renegociadas o novadas, o estas se encuentren con alguna modalidad pendiente;

— aquellas exceptuadas en razón de **circunstancias personales** del titular: las que se originan en un periodo de cesantía de su titular;

— las exceptuadas en razón del **tiempo transcurrido:** aquellas morosidades de la persona respecto de las cuales han transcurrido cinco años desde que la respectiva obligación se hizo exigible, y

— aquellas que se **han extinguido:** ya sea porque han sido pagadas o se han extinguido por otro modo legal, una vez transcurridos los 5 años desde que la obligación se hizo exigible.

Esto último se entiende porque, de acuerdo al artículo 19 de esta misma ley, "el pago o la extinción de estas obligaciones por cualquierotro modo produce la caducidad o la pérdida de fundamento legal de los datos respectivos para los efectos del artículo 12, mientras estén pendientes los plazos que establece el artículo precedente".

La Ley Nº 19.628 dispone que es dato caduco "el que ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia o, si no hubiese norma expresa, por el cambio de los hechos o circunstancias que consigna" (art. 2º letra d, Ley Nº 19.628).

Un solo dato responderá con veracidad a la situación de su titular: el dato relativo a una obligación impaga que se encuentra en mora, que no se ha extinguido por algún medio legal y a cuyo respecto no se ha cumplido el plazo o la condición impuesta por el legislador para el cese de su tratamiento o para su comunicación.

Un solo dato responderá con veracidad a la situación de su titular: el dato relativo a una obligación impaga que se encuentra en mora, que no se ha extinguido por algún medio legal y a cuyo respecto no se ha cumplido el plazo o la condición impuesta por el legislador para el cese de su tratamiento o para su comunicación.

Si el dato es caduco, surge la obligación de eliminar o cancelar los datos personales del banco de datos, sin que sea necesario el requerimiento del titular. Así por ejemplo, no podrá incluirse en la fórmula de cálculo de un predictor de riesgo comercial. Asimismo, consideramos que el artículo 18 de la ley en análisis reconoce este requisito cuando dispone:

> "En ningún caso pueden comunicarse los datos a que se refiere el artículo anterior, que se relacionen con una persona identificada o identificable, luego de transcurridos cinco años desde que la respectiva obligación se hizo exigible.

Tampoco se podrá continuar comunicando los datos relativos a dicha obligación después de haber sido pagada o haberse extinguido por otro modo legal.

Con todo, se comunicará a los tribunales de justicia la información que requieran con motivo de juicios pendientes".

4.5.1.3 Razonabilidad

Más allá de la idoneidad y pertinencia de los datos personales que sean objeto de tratamiento, la razonabilidad en materia de calidad del tratamiento de datos dice relación con el cumplimiento de las reglas y procedimientos generalmente aceptados (estándares) en el ámbito del que se trate.

A vía ejemplar, si lo que pretendemos es realizar un tratamiento de datos para efectos de evaluar el riesgo comercial de una persona o su solvencia económica, deberemos considerar las normas técnicas derivadas de la ciencia estadística que han modelado los predictores a partir de antecedentes que sean útiles y eficaces para la predicción del comportamiento de pago futuro, además de las normas relativas a información que legítimamente se puede agregar a los motores de cálculo, de forma tal que se obtenga el mayor beneficio desde el punto de vista de las necesidades del sector financiero y con el menor daño a los derechos de las personas.

Tratándose del tratamiento de datos personales con finalidades sanitarias, para evaluar los factores que afectan la salud de la población será la ciencia médica la que otorgará los parámetros a considerar, y así sucesivamente.

4.5.2 Proporcionalidad

Este principio implica que el tratamiento de datos de carácter personal deberá circunscribirse a aquellos que resulten **adecuados, pertinentes y no excesivos** en relación con las finalidades previstas de acuerdo al principio recién analizado.

En particular, la persona responsable deberá realizar esfuerzos razonables para limitar los datos de carácter personal tratados al mínimo necesario.[88] Por tanto, se entenderá que se cumple con el principio de proporcionalidad cuando exista:

a. **Idoneidad:** el o los datos que se recolecten, así como su posterior tratamiento, son adecuados o apropiados a la finalidad que motiva la recogida.

b. **Proporcionalidad:** los datos son pertinentes, relevantes o conducentes y no excesivos en relación a la referida finalidad.

Veamos un ejemplo.

Para cumplir con el principio de proporcionalidad en el otorgamiento de un crédito de consumo, un banco podrá recabar los antecedentes relativos a la identificación del solicitante, sus antecedentes comerciales y demás necesarios para verificar la concurrencia de los requisitos establecidos para el otorgamiento, los cuales en todo caso deben estar relacionados con la naturaleza del crédito.

En aplicación de este principio, el responsable del tratamiento deberá optar, de entre los diversos tratamientos que le permitan conseguir los fines pretendidos, por aquel que menor incidencia tenga en el derecho a la protección de datos personales y por la utilización de los medios menos invasivos.

A vía ejemplar, un banco cumple con el principio de proporcionalidad en el proceso de otorgamiento de un crédito de consumo si solo incluye, en el proceso de análisis, los datos personales que el cliente (titular de datos) comunicó voluntariamente o autorizó a que el banco solicitara a terceros, o en su defecto que ya consten en sus bases de datos en virtud de la historia contractual entre el banco y ese cliente.

88 Cfr. Resolución de Madrid; p. 11.

Adicionalmente, estos datos deberán corresponder a las políticas de riesgo crediticio del banco[89], en la medida que dichos datos se encuentran relacionados directamente con datos de solvencia patrimonial y crédito del cliente, y que los algoritmos de análisis sean transparentes y no discriminatorios.

4.5.3 Temporalidad del tratamiento

La Ley Nº 19.628, en materia de temporalidad, solo considera la regla relativa a los datos sobre morosidades, que vimos antes y según la cual los datos solo podrán comunicarse hasta un máximo de 5 años desde que la obligación se hizo exigible.

Una interpretación sistémica de la ley nos permite sostener que la legitimidad del tratamiento de datos se mantiene por el tiempo que sea necesario para cumplir con la finalidad que motivó la recolección, más allá de lo cual los datos debieran ser anonimizados.

Sin perjuicio de lo anterior, una interpretación sistémica de la ley nos permite sostener que la legitimidad del tratamiento de datos se mantiene por el tiempo que sea necesario para cumplir con la finalidad que motivó la recolección, más allá de lo cual los datos debieran ser anonimizados.

En derecho comparado, ya el Convenio Nº 108 exigía que los datos debían ser conservados en forma tal que permita la identificación de los interesados durante un plazo que no excediere del necesario para los fines para los que fueron registrados.

Una solución genérica se justifica porque no siempre es posible, *a priori* y en términos genéricos, establecer el plazo por el cual podrán mantenerse los datos personales identificados, sino que eso deberá analizarse en cada caso concreto. Más adelante nos referiremos al derecho al olvido como una de las vías de reclamación contra el tratamiento de datos personales más allá del tiempo razonable.

89 Ver artículos 17A a 17G de la Ley Nº 19.496 sobre protección de los derechos de los consumidores, como también el Manual de Requerimiento de Información al Proveedor, del Servicio Nacional del Consumidor (Sernac).

4.5.4 Calidad de proceso

Los procesos asociados al tratamiento de datos deben ser de calidad y ello implica, al menos, contar con una política de privacidad que se haga cargo de:

- que se definan perfiles de acceso y privilegios que den cuenta de la función de cada una de las personas que entra en contacto con los datos personales;
- que se adopten las medidas de seguridad de fuga de datos (ej. bloqueo de puertos USB o control de copias de archivos en memorias flash, medidas de control de archivos enviados a través de correos públicos de funcionarios);
- sistemas de trazabilidad de los datos personales relativo a los tratamientos que hayan hecho los funcionarios o terceros respecto de los datos;
- documentación de las reglas de negocio para dar cumplimiento al principio de transparencia;
- documentación de reglas y procedimientos de tratamiento de datos para responder a eventuales ejercicios de derechos de titulares de datos;
- documentación e implementación de reglas y procedimientos de detección y mitigación de incidentes de seguridad de datos;
- segmentación de datos y permisos por procesos asociados a productos y servicios;
- adecuación de los contratos de trabajo para la inclusión de cláusulas relativas al deber de secreto en el tratamiento de datos por parte de los trabajadores, y
- capacitaciones permanentes a los cuadros funcionarios en el tratamiento adecuado de los datos.

4.5.5 Cumplimiento de derechos de los titulares de datos

Se cumplirá con esta exigencia si el titular del registro o banco de datos dispone de todas las medidas necesarias para que el interesado pueda ejercer sus derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos.

Asimismo, implica el establecimiento de los mecanismos que le permitan reclamar, ante el organismo de control pertinente, acerca de las decisiones del responsable del registro, o de terceros, que puedan afectarle o vulnerar sus derechos.

Recordemos que los plazos de respuesta a los requerimientos de los titulares son muy acotados, pues la ley le otorga solo 2 días para hacerlo.

4.6 Principio de control

Este principio exige que existan mecanismos para comprobar que la actividad del responsable del registro o banco de datos personales se lleva a cabo acorde a los principios generales y normas que rigen el tratamiento de datos personales.

Este control podrá ser ejercido por el interesado a través de los derechos que se le reconocen, o a través de una agencia pública o autoridad de control, concebida como un órgano independiente encargado de vigilar la aplicación de las normas de protección de datos.

Respecto del origen de este principio, se debe reiterar que su primera manifestación se encuentra en el Proyecto Baker. Sin embargo, debe destacarse que es el Proyecto Huckfield (1971), titulado *Control of Personal Information*, el que establece claramente entre sus motivaciones la creación de un tribunal y una inspección de bancos de datos que contengan información de carácter personal, a fin de tomar todo tipo de medidas para prevenir el abuso de las informaciones memorizadas en los bancos de datos, sean estos manuales o informáticos.

Entre las **atribuciones** que debieran tener las autoridades de control, se incluyen las **consultivas**, respecto de las autoridades públicas y para el sector privado, en las materias técnicas asociadas a la aplicación práctica de la normativa de protección de datos y su perfeccionamiento. En segundo lugar, poderes de **investigación** en términos tales que pueda recabar toda la información necesaria para el cumplimiento de su misión de control.

En tercer lugar, se le reconocen a la autoridad de control poderes de **intervención**, ya sea autorizando antes de realizar los tratamientos, impartiendo instrucciones en los distintos sectores o materias en las cuales se realizan tratamientos de datos, además de ordenar el bloqueo, la supresión o la destrucción de los datos, prohibir provisional o definitivamente un tratamiento, dirigir una advertencia o amonestación al responsable del tratamiento, o someter la cuestión a los tribunales de justicia u otras autoridades, si es del caso.

Sobre las materias de que conoce la autoridad de control, cualquiera sea la denominación que tome en cada Estado, comprende el conocimiento de las solicitudes que cualquier persona o cualquier asociación que la represente, interponga en relación con la protección de sus derechos y libertades respecto del tratamiento de datos personales.

En este punto, cabe destacar las atribuciones jurisdiccionales de la autoridad de control. En efecto, esta podrá conocer de infracciones a la ley y ponerlas en conocimiento de la autoridad judicial.

Sobre las materias de que conoce la autoridad de control, cualquiera sea la denominación que tome en cada Estado, comprende el conocimiento de las solicitudes que cualquier persona o cualquier asociación que la represente, interponga en relación con la protección de sus derechos y libertades respecto del tratamiento de datos personales. Especialmente, conocerá las solicitudes de verificación de la licitud de un tratamiento de datos personales.

Una vez presentada la solicitud y en todo caso, debe informar al solicitante acerca del curso dado a su petición.

En cuanto a la **competencia territorial** de la autoridad de control, se entiende que será competente para ejercer sus atribuciones en todo el territorio del Estado o, en algunos casos, en una región o materia específica.

Analizadas las atribuciones de la autoridad de control, y como contrapartida, debemos hacer mención a las **obligaciones** que normalmente afectan a este organismo.

Al respecto, y en primer lugar, es importante señalar que este organismo debe **rendir informes** sobre sus actividades, los que debieran ser públicos; y en segundo lugar, en lo que respecta a la responsabilidad de las personas naturales que integran la autoridad de control, se estima que los miembros y agentes de las autoridades de control debieran estar sujetos, incluso después de haber cesado en sus funciones, al deber de **secreto profesional** sobre informaciones confidenciales a las que hayan tenido acceso, previéndose un tiempo en el cual no debieran poder trabajar en las empresas u organismos respecto de los cuales le correspondió pronunciarse durante el ejercicio de sus funciones.

Finalmente, y no por ello menos importante, cabe destacar el deber de **cooperación o colaboración** entre las distintas autoridades de control, en la medida necesaria para el cumplimiento de sus funciones, en particular mediante el intercambio de información que estimen

útil. A vía ejemplar, a nivel iberoamericano, la Red Iberoamericana de Protección de Datos (RIPD) agrupa y propicia la cooperación de las agencias nacionales de este entorno.

Deberes legales especialmente exigibles

← Índice de contenidos

5.1 Deber de seguridad en el tratamiento de datos personales

En cumplimiento del deber de seguridad, el responsable del tratamiento de datos personales debe aplicar las medidas técnicas y organizativas necesarias para el adecuado resguardo de la integridad, disponibilidad o acceso debido de los datos personales[90], en los niveles razonablemente necesarios para garantizar el equilibrio entre el costo de la medida y nivel de sensibilidad de los datos objeto del tratamiento.

Estos deberes son de responsabilidad del titular del banco de datos personales, con independencia de que realice el tratamiento por sí o a través de un tercero.

El Reglamento Europeo (RGPD) especifica que los datos personales deben ser "tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas (integridad y confidencialidad)", previendo a este respecto que el responsable del tratamiento será responsable también de demostrar el cumplimiento de ese deber (responsabilidad proactiva).[91]

90 A vía de ejemplo, el artículo 17 Directiva 46/95 CE disponía que, en cumplimiento de este principio, se deberá "aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental o contra la alteración, la difusión o el acceso no autorizado, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales". De su parte, el art. 7º del Convenio Nº 108, 1981 CE, dispone que "las medidas de seguridad oportunas para proteger los datos de carácter personal registrados en archivos automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, modificación o difusión no autorizados".

91 Reglamento (UE) 2016/679, art. 5 Nº 1 letra f y Nº 2.

El legislador chileno, dispone que el responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños, comprendiendo tanto el daño patrimonial como el daño moral.

El legislador chileno, a este respecto, dispone que el responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños[92], comprendiendo tanto el daño patrimonial como el daño moral.

De su parte, las personas que trabajan en el tratamiento de datos personales, tanto en organismos públicos como privados, están obligadas a guardar secreto sobre los mismos cuando provengan o hayan sido recolectados de fuentes no accesibles al público, y sobre los demás datos y antecedentes relacionados con el banco de datos, obligación que no cesa por haber terminado sus actividades en ese campo.[93]

Por ejemplo, es atingente a la seguridad del tratamiento de datos personales el buen funcionamiento de las medidas de seguridad física y lógica, tales como las políticas de clave, la definición de perfiles de acceso a la información, la trazabilidad de la información, los registros que van dejando constancia en el sistema de quiénes han consultado los datos o han realizado reportes con ellos datos, con señalamiento de día, hora y respuesta entregada, etcétera.

En virtud de este principio los responsables del tratamiento deberán "aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental o contra la alteración, la difusión o el acceso no autorizado, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales", en los niveles de razonabilidad necesarios para garantizar el equilibrio entre el costo de la medida y nivel de sensibilidad de los datos objetos del tratamiento.

Esta norma resulta más específica que aquella contenida en el Convenio Nº 108, que señala que "las medidas de seguridad oportunas para proteger los datos de carácter personal registrados en archivos

92 Artículo 11, Ley Nº 19.628.
93 Artículo 7º, Ley Nº 19.628.

automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, modificación o difusión no autorizados".

Cuando el tratamiento sea llevado a cabo por un tercero al que el responsable del tratamiento le ha encargado esta tarea, se exige en primer lugar que el responsable, al momento de elegir al encargado, escoja a aquel que reúna las garantías suficientes en relación con las medidas de seguridad técnica y de organización de los tratamientos que deban efectuarse. Además, debe asegurarse de que se cumplen dichas medidas y de que la realización del tratamiento por encargo esté regulada por un contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable de este, que se haga constar por escrito o en otra forma equivalente, a efectos probatorios y que disponga, en particular, que el encargado del tratamiento solo actúa siguiendo instrucciones del responsable del tratamiento y que las obligaciones del apartado 1, tal como las define la legislación del Estado miembro en el que esté establecido el encargado, incumben también a este.

Una de las tareas a desarrollar en la planificación de un proceso de tratamiento de datos personales es el establecimiento de un plan general de seguridad que contemple los posibles riesgos, tanto técnicos como personales o aun ambientales, a los que está expuesto el registro o banco de datos.

No debemos olvidar que estamos en el contexto de una sociedad en que los datos se han constituido en un bien transable en el mercado. En efecto, nos enfrentamos al comercio de la información, que ha merecido una especial consideración de parte del legislador atendida la importancia que ha cobrado con el correr del tiempo.

Atendiendo lo anterior y respecto de las medidas de seguridad en general, se ha señalado que una de las tareas a desarrollar en la planificación de un proceso de tratamiento de datos personales es, precisamente, el establecimiento de un plan general de seguridad que contemple los posibles riesgos, tanto técnicos como personales o aun ambientales, a los que está expuesto el registro o banco de datos.

Asimismo, se deberá designar un encargado de seguridad, en quien radicará el efectivo cumplimiento de este plan, de manera que no se produzcan siniestros y, si se producen, aminorar al máximo sus consecuencias.

A vía de enunciación, podemos señalar que un plan de seguridad pretende evitar el deterioro o inutilización de equipos e instalaciones (seguridad física); el deterioro o destrucción de programas y los archivos computacionales en los cuales consta el registro o banco de datos (seguridad lógica); las interrupciones del servicio o el funcionamiento degradado de equipos y sistemas (disponibilidad de medios); los errores en los procesos o las pérdidas de información (integridad de los datos o programas); el mal uso de los medios o la utilización ilícita de los mismos, ya sea del personal como de terceros, y la difusión o salida al exterior de informaciones consideradas confidenciales o la interceptación ilegítima en los procesos de transmisión de los datos.

Este último objetivo tiene mucho que ver con lo que al respecto pueda decir el derecho de las telecomunicaciones, ya que al operar procesos de transmisión de información, el establecimiento de las medidas de seguridad será una tarea compartida entre los responsables de los registros y bancos de datos y la autoridad pública en quien radique el servicio público de telecomunicaciones.

También habrá de mencionarse, en este punto, la existencia de mecanismos de seguridad, tales como la firma electrónica y la encriptación de mensajes, los cuales serán útiles al momento de garantizar la seguridad en la transmisión de información.

5.2 Protección de datos desde el diseño

El proyecto de reforma de la Ley Nº 19.628 busca establecer el deber de incluir las reglas de protección de datos desde el diseño de los proyectos de bases de datos y luego, en su concreción, que la protección de los datos sea la que se habilita en los sistemas "por defecto", en los siguientes términos:

> "**Deber de protección desde el diseño y por defecto**. El responsable debe aplicar medidas técnicas y organizativas apropiadas con anterioridad y durante el tratamiento de datos con el fin de cumplir los principios del tratamiento de datos y los derechos de titular establecidos en esta ley. Las medidas deben ser adoptadas considerando el estado de la técnica, los costos de implementación y la naturaleza, ámbito, contexto y fines del tratamiento de datos, así como los riesgos.
>
> El responsable de datos deberá aplicar las medidas técnicas y organizativas para garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para los fines específicos y determinados del tratamiento. Esta obligación se aplicará al número de datos recogidos, a la extensión del tratamiento, al plazo de conservación de los datos y a su accesibilidad".

Esta norma se basa en lo previsto en el Reglamento europeo de protección de datos. Al respecto, el considerando 78 del RGPD recoge una cuestión que había sido objeto de debate en el ámbito académico, como es el hecho de que la protección de los derechos y libertades de las personas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas desde el inicio, desde que la organización plantea la necesidad de generar un registro o banco de datos.

Es decir, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de la protección de datos personales desde el diseño y por defecto.

Ello implicaría que al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de procurarse que los productos, servicios y aplicaciones tengan en cuenta el derecho a la protección de datos y que garanticen, con la debida atención al estado de la técnica, que los responsables y los encargados del tratamiento que reciban esas aplicaciones, productos y servicios puedan cumplir sus obligaciones legales en la materia.

Más todavía, el Reglamento pretende que los principios de la **protección de datos desde el diseño y por defecto** también deban tenerse en cuenta en el contexto de los contratos públicos, como en las compras públicas y los llamados a licitación. Incluso, prevé que para garantizar todo lo anterior se generen mecanismos de certificación técnica. El artículo 25, número 2, lo expresa así:

> "El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas".

Cuando hablamos de protección de datos por diseño, nos referimos a la incorporación de las reglas de protección de datos personales desde la fase inicial de un proyecto tecnológico que considere el tratamiento de datos personales.

Esta obligación no es más que el reconocimiento del principio de calidad y la responsabilidad del responsable del registro o banco de datos. En efecto, para que se dé cumplimiento a estos imperativos, desde el diseño del registro o banco de datos deben considerarse las facultades legales, la finalidad, a quién se comunicarán los datos, qué datos serán objeto de tratamiento, y todos aquellos elementos que permitan luego demostrar que se ha actuado con la debida diligencia.

Cuando hablamos de protección de datos por diseño, nos referimos a la incorporación de las reglas de protección de datos personales desde la fase inicial de un proyecto tecnológico que considere el tratamiento de datos personales. Este concepto ha sido incorporado

en el RGPD que se aprobó en Europa en 2016 y que entró en vigor el 25 de mayo de 2018. En su artículo 25 lo establece como "el derecho a la protección de datos desde el diseño y por defecto".[94]

Al referirse al diseño, el reglamento dispone que los responsables del tratamiento deberán incorporar "medidas técnicas y organizativas apropiadas, como la seudonimización[95], concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados".

A su vez, "por defecto" implica que "solo sean objeto de tratamientolos datos personales que sean necesarios para cada uno de los finesespecíficos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminadode personas físicas".

94 RGPD: "Artículo 25. Protección de datos desde el diseño y por defecto.
1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.
2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.
3. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo".

95 La opinión 05/2014, del Grupo de trabajo sobre protección de datos personales del Artículo 29 (WP29), sobre técnicas de anonimización en la web, en su número 4 se refiere a la seudonomización como "la sustitución de un atributo (normalmente un atributo único) por otro en un registro. Por consiguiente, sigue existiendo una alta probabilidad de identificar a la persona física de manera indirecta; en otras palabras, el uso exclusivo de la seudonomización no garantiza un conjunto de datos anónimo"... para agregar luego que "La seudonomización reduce la vinculabilidad de un conjunto de datos con la identidad del interesado; se trata por tanto de una medida de seguridad útil, pero no es un método de anonimización"

Partiendo del análisis anterior podemos referirnos a una *smart data protection*, esto es protección de datos inteligente, que considere las circunstancias especiales de cada una de las personas que son titulares de datos y la naturaleza de la relación que legitima el tratamiento de datos, para los efectos de que se haga realidad el imperativo según el cual toda persona tiene derecho a controlar los usos que terceros dan a la información que le concierne (autodeterminación informativa).

En el ámbito canadiense, Cauvoukian consideró que la privacidad por diseño se basa en los siguientes **siete principios**[96], que debieran ser integrados en la arquitectura de los sistemas que tratan datos personales.

5.2.1 Proactivo, no reactivo ni remedial

En lo que nos interesa, el modelamiento mismo del contrato inteligente evalúa y considera los posibles riesgos de intrusiones ilegítimas y afectaciones a la privacidad, antes de que estos se materialicen.

El sistema está diseñado para reunir y conservar evidencia, monitorea el comportamiento de los usuarios para detectar anomalías, adopta prácticas de seguridad estrictas, con altos niveles de protección, de acuerdo a los más altos estándares legislativos, técnicos y organizativos.

5.2.2 Privacidad como configuración determinada o por defecto

La arquitectura de sistema debiera tener la configuración de las reglas de privacidad más estrictas que deban aplicarse a cada dato personal que es objeto de tratamiento, sin necesidad de que el usuario haga algo. Consecuentemente, debe preverse la posibilidad de que sea el usuario quien opte por bajar los niveles de seguridad.

Desde el punto de vista del análisis del caso, en un juicio en que se debata la responsabilidad por el tratamiento de datos personales, los siguientes ejes de análisis nos permitirán determinar si el responsable de la base de datos actuó con la debida diligencia. Asimismo, en un

96 CAVOUKIAN, Ann: *Privacy by Design. The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices*. Disponible en línea [consulta: 21.09.2020].

juicio por responsabilidad contractual, nos permitirán verificar si el proveedor cumplió con sus deberes contractuales y legales en el desarrollo de los sistemas.

Nombre del indicador	Descripción	Evidencias
Especificación de propósito	La finalidad con que los datos son recogidos, almacenados y tratados debe ser legítima e informada al titular de los datos antes de su recogida, y en los casos que proceda deberá recabarse su consentimiento.	— En documentación del proyecto consta finalidad del tratamiento. — En la documentación destinada a los usuarios se informa del tratamiento y su finalidad. — Constatación del fundamento legal: consentimiento o autorización legal.
Limitación de la recogida	Los datos que se recolecten deben ser estrictamente los necesarios para satisfacer el propósito declarado y, en su caso, consentido por el titular de los datos personales.	— Existen procesos detallados en que consta qué datos personales se utilizan en cada uno de ellos. — Existe segregación de funciones y limitaciones de acceso a los datos por perfiles asociados a competencias/procesos.
Minimización de datos	Una vez que constan en el sistema, los datos "identificados" o "reidentificables" que se mantengan serán los estrictamente necesarios para satisfacer el propósito. En los demás casos se aplicarán métodos de cancelación, anonimización o de seudonimización.	— Las políticas y procesos de tratamiento de datos contemplan mecanismos de desidentificación de los datos. — En los procesos de contratación con proveedores se consideran cláusulas de confidencialidad. — Los procesos señalan los datos que se requieren en cada proceso. — Los mecanismos de recogida de datos se diseñan para obtener los datos estrictamente necesarios. — No existen bodegas de datos no asociados a finalidades legítimas e informadas.
Limitación en la retención de datos	El tiempo de almacenamiento de datos queda condicionado al propósito del tratamiento y respeta las limitaciones legales.	— Los datos relativos a información sobre morosidades de la persona se mantiene hasta un máximo de 5 años desde que la obligación se hizo exigible. — Se implementan mecanismos de cancelación de datos en las hipótesis de caducidad. — Los datos asociados a un contrato se mantienen desde la fase precontractual y hasta la plena ejecución del contrato. — No existen bodegas de datos históricos.
Precaución o enfoque de riesgos	En los casos que exista duda sobre el carácter privado o público de la información, por defecto el sistema debe optar por las reglas más estrictas.	— Se realizan auditorías periódicas enfocada a identificar brechas de procesos o de sistemas. — Se cuenta con certificaciones de procesos. — Si un sistema trata de manera conjunta datos sensibles y datos simplemente personales, se aplican a todos ellos reglas de seguridad estrictas. — Se cuenta con inventarios de datos personales de acuerdo a su sensibilidad.

Arquitectura enfocada a la protección de datos	El registro o banco de datos, en todas sus etapas de desarrollo y operación, debe considerar las reglas de tratamiento de datos personales de forma que se logre la finalidad del tratamiento con el mínimo riesgo en la protección de datos.	— Las interconexiones con sistemas de borde tienen respaldo legal y contractual (ej. en un sistema de apoyo a contratos, la integración con el banco, con el SII, con las bodegas de despacho, etc.). — Existen mecanismos de auditoría de los sistemas. — Se prevén certificaciones de procesos y de seguridad.
Evaluación de impactos[97]	Se realizan evaluaciones de impacto tanto en la aceptación social del sistema como en la determinación de los efectos del tratamiento de datos en los derechos de las personas.	— Existen documentos del proceso y resultados de la evaluación de impacto. — Documentos del proyecto muestran que este se ajusta a los resultados de la evaluación. — Se realizan evaluaciones periódicas de los efectos del tratamiento de datos en los derechos de las personas y en la satisfacción de la finalidad. — Se aplican test de daños.
Auditabilidad	Tanto la documentación del sistema como el sistema mismo deben ser susceptibles de revisión de acuerdo a metodologías de seguridad de la información, para poder detectar cualquier desviación, ya sea de la finalidad o propósito, destinatarios y/o procesos en los cuales se usen los datos personales.	— El sistema cuenta con políticas de privacidad. — Se cuenta con inventario de datos personales. — Los datos personales se etiquetan. — Se realizan auditorías independientes de los sistemas. — Existen fiscalizaciones de organismos reguladores que se pronuncian sobre los procesos y sistemas. — Se prevé la certificación de los sistemas y procesos. — Se han designado responsables del tratamiento de datos personales. — Existe documentación del proyecto y da cuenta de los procesos, datos y resguardos a implementar — Las políticas de uso y términos generales se publica y se encuentran accesibles a los usuarios finales. — Se han aplicado multas por incumplimiento de las condiciones legales o contractuales. — Se documentan los consentimientos de los titulares de datos.

97 Agencia Española de Protección de Datos. Guía para una evaluación de impacto de la protección de datos personales. 2014. Disponible en línea, define la evaluación de impacto como "un ejercicio de análisis de los riesgos que un determinado sistema de información, producto o servicio puede entrañar para el derecho fundamental a la protección de datos de los afectados y, tras ese análisis, afrontar la gestión eficaz de los riesgos, identificándolos mediante la adopción de las medidas necesarias para eliminarlos o mitigarlos".

Seguridad de extremo a extremo	La seguridad de la información debe guiar todo el ciclo de vida de los datos personales, garantizándose su confidencialidad, integridad y disponibilidad.	— Se implementan mecanismos seguros de recogida, procesamiento, comunicación, modificación y destrucción de datos personales. — Se implementan mecanismos de cifrado de la información. — Se considera segregación de funciones. — Se cuenta con seguros de responsabilidad. — Se exige certificaciones de seguridad a los proveedores. — Se han incluidos cláusulas de confidencialidad y seguridad en los contratos. — Se realizan auditorías de seguridad y *hacking* ético. — Se implementan políticas y procesos de seguridad de la información. — Existe una estructura de perfiles y cargos asociadas a la seguridad de la información. — Se implementan procesos seguros.
Responsabilidad	Se implementan los procesos asociados al cumplimiento de obligaciones legales	— Se han implementado los derechos de acceso, rectificación, supresión o cancelación, oposición y portabilidad de los datos personales. — En los procesos de comunicación de datos a terceros, se verifican las hipótesis de legalidad (competencias del receptor, finalidad del tratamiento declarada). — Se deja trazabilidad de los procesos asociados a los datos personales. — Se implementan procesos de cancelación de datos caducos. — Existe un encargado del tratamiento de datos. — Los perfiles de acceso a los datos personales son auditables. — Se implementan procesos de comunicación de incidentes relativos a datos personales. — Existen procedimientos de cambio asociado a modificaciones legales.

El Consejo para la Transparencia debió pronunciarse en amparo C-2493-2015, respecto de la siguiente solicitud de acceso a la información pública: "Acceder a todos los antecedentes relativos a la enfermedad silicosis pulmonar durante los años 2014-2015 en Valparaíso". Se solicitaba que se adicionaran a la respuesta todos los antecedentes relativos a los trabajadores que sufren dicha enfermedad, así como todas las pensiones de invalidez de la Ley Nº 19.744 por silicosis pulmonar otorgadas durante 2014 y 2015, y envío de copia en formato PDF de todas las resoluciones emitidas por la Comisión de Medicina Preventiva e Invalidez (Compin), la Comisión Médica de Reclamos (Comere) o la Superintendencia de Seguridad Social (Suseso).

Es del caso que el organismo requerido, en aplicación del principio divisibilidad consagrado en el artículo 11 letra e de la ley de transparencia y, de paso, cumpliendo las reglas de la privacidad desde el diseño, en la respuesta si bien entregó al solicitante 35 resoluciones, tarjó los datos personales sin solicitar a los titulares de datos si consentían en la entrega de sus identidades, lo que motivó la interposición del amparo.

El Consejo, por unanimidad rechazó el amparo dado que "el estado de salud de las personas constituye un dato sensible cuya divulgación se encuentra prohibida". Tal decisión fue objeto de reclamo de ilegalidad ante la Corte de Apelaciones de Santiago, en autos rol Nº 5833-2016. A continuación transcribimos los considerandos que estimamos relevantes para la comprensión de la resolución de rechazo:

> "Segundo: que basta para desestimar el reclamo de autos, tener presente que si bien la Ley de Transparencia no exige precisar la finalidad del uso de la información solicitada, en la especie -tal como han hecho presente la Secretaría Regional Ministerial de Valparaíso y el Consejo para la transparencia, don Sebastián Riesco en su solicitud (fojas 1) explicó que realizaba un artículo académico respecto de la silicosis en Chile y que con el objeto de poder concluir dicho trabajo necesitaba contar con información de respaldo

'estadístico' de la situación actual de la enfermedad en Chile, de modo que atendiéndose a lo dispuesto en el artículo 2 letra e) de la ley 19.628 sobre Protección de Datos de Carácter Personal, ningún agravio se ocasiona al recurrente al otorgar la información en la forma que ahora impugna, guardando completa coherencia lo solicitado con lo concedido, por cuanto al tratarse de un 'dato estadístico' en su origen o como consecuencia de su tratamiento no puede ser asociado a un titular identificado o identificable".

"Quinto: Que, de su parte, en lo que atañe al procedimiento y específicamente a lo dispuesto por el artículo 20 de la ley 20285 y 10 de la ley 19.629, en concepto de esta Corte la notificación a terceros que echa de menos el recurrente es obligatoria cuando pueden verse afectados sus derechos patrimoniales, más no sus datos sensibles, como acontece en la especie, toda vez que el deber de reserva de datos sensibles es un bien superior lo que se traduce en que la notificación no se erige en una exigencia para rechazar la entrega, máxime su la información de estado de salud de una persona, no es información pública, sino que esencialmente privada e íntima, por lo que aquella información es privativa de su titular y lo único que puede ser de interés general es el antecedente genérico que puede extraerse para fines estadísticos, nada más, constituyendo una excepción la utilización y conocimiento de los datos sensibles por las instituciones que la ley autoriza para los fines que el ordenamiento jurídico prevé y que se relacionan con el manejo, prevención, contención y tratamiento de ciertas enfermedades, evento en el cual los datos sensibles siguen siendo reservados para el resto de la población".

5.3 Evaluaciones de impacto y consulta previa

En general se habla de evaluación de impacto cuando se quiere medir y establecer la diferencia respecto de alguna variable que se ha escogido como indicador de resultado de una intervención en un ámbito específico.

El Banco Mundial[98] señala que la evaluación de impacto se centra en la formulación de políticas basadas en evidencias. Para ello se considera modelos de monitoreo de un "objeto", basados en indicadores cuantitativos y/o cualitativos. Si bien esta aproximación corresponde a la evaluación de programas o proyectos, creemos importante tenerlas a la vista en el presente análisis.

En materia de protección de datos, la Agencia Española de Protección de Datos[99] ha recogido varios conceptos, sin embargo estos solo describen el proceso que se lleva a cabo para evaluar los impactos del tratamiento de datos, sin aportar elementos que permita tomar conocimiento sobre el sentido y alcance de esta metodología, la cual busca proporcionar herramientas "que las partes interesadas pueden utilizar para verificar y mejorar la calidad, la eficiencia y la efectividad de las intervenciones en varias etapas de la implementación".[100]

La evaluación debiera aplicarse a todo el ciclo de vida de un proyecto, desde su formulación y mientras se mantenga operativo, incluso luego de su extinción, aportando información objetiva sobre el diseño, ejecución y resultados, que permita a los órganos directivos y operativos del proyecto obtener retroalimentación para corregir los efectos adversos o posibles desviaciones del proyecto.

98 Banco Mundial/Banco Internacional de Reconstrucción y Fomento. *La evaluación de impacto en la práctica*. Documento elaborado por Paul Gertler, Sebastián Martínez, Patrick Premand, Laura B. Rawlings, Christel M.J. Vermeersh, 2011. ISBN 978-0-8213-8541-8; p. 22. Disponible en línea [consulta: 12.09.2021].

99 Agencia Española de Protección de Datos. *Guía para una evaluación de impacto en la protección de datos personales*. Madrid, 2014; pág. 8

100 Banco Mundial/Banco Internacional de Reconstrucción y Fomento. *La evaluación de impacto en la práctica*. Documento elaborado por Paul Gertler, Sebastián Martínez, Patrick Premand, Laura B. Rawlings, Christel M.J. Vermeersh, 2011. ISBN 978-0-8213-8541-8. Disponible en línea [consulta: 12.09.2021].

La evaluación de impacto en la protección de datos podría definirse como una metodología que permite verificar el efecto causal en los derechos y libertades de la persona ocasionado por o con ocasión del tratamientos de datos personales.

En lo que nos interesa, la evaluación de impacto es útil en los recursos de protección en que los afectados por el tratamiento consideran que el responsable del banco de datos personales, de manera arbitraria e ilegal, ha desarrollado un determinado proceso de tratamiento de datos personales.

En este sentido, la evaluación de impacto en la protección de datos podría definirse como una metodología que permite verificar el efecto causal en los derechos y libertades de la persona ocasionado por o con ocasión del tratamientos de datos personales.

Si bien en la fase de proyecto se trata de anticiparse a los efectos directos que tendrá en los derechos y libertades de la persona, y utilizaremos este indicador para demostrar la debida diligencia, no es menos cierto que muchos proyectos de tratamiento de datos no han contemplado esta actividad, por lo que corresponderá *a posteriori* verificar si el tratamiento de datos lesiona los derechos de las personas o se encuentra dentro de los límites de lo aceptable.

La consagración del derecho a la protección de datos busca que la realización de una operación de tratamiento de datos personales cumpla con la finalidad legítima e informada, siendo a la vez sea lo menos dañina posible para los derechos de las personas. A continuación, algunas preguntas que podría hacerse el analista frente a un determinado conflicto por esta materia.

Pregunta	Resultado
¿La finalidad del tratamiento es legítima?	Del análisis de la legislación vigente se podrá determinar si se cumplen las hipótesis de legalidad del tratamiento de datos.
¿Qué procesos o actividades requerirán datos personales?	El mapa de procesos y actores que accederán a los datos personales en cada una de las fases es coherente con los roles que desempeñarán en relación a los datos y las decisiones que se adoptan o las respuestas que da el sistema en cada etapa.
¿Qué normativa rige la materia y cómo se aplica al caso concreto?	El análisis en detalle de la normativa que rige la actividad de tratamiento aplicada al caso concreto muestra o no el cumplimiento de las condiciones legales en cada etapa.
¿Qué efectos se produce en los derechos y libertades por ese conjunto de tratamiento de datos?	En cada fase del proceso, se analizará el resultado en relación a los derechos de la persona. A vía ejemplar, la inclusión de un criterio X en la evaluación de riesgo comercial de un cliente redundará en la decisión sobre si contratar o no con esa persona, o en el precio a cobrar, con un efecto directo en la libertad de contratación de esa persona y,

	eventualmente, un efecto indirecto en otros derechos que se pretendía satisfacer con el contrato proyectado, tales como la salud, a la educación, la alimentación, la comunicación, etc. Ciertamente, la evaluación solo debería considerar los efectos directos.
¿Cuál es el tratamiento de datos que tiene la misma eficacia con el mejor perjuicio a los derechos y libertades de las personas afectadas por el tratamiento?	Si hay varias formas de obtener el mismo resultado, deberá optarse por aquella que produzca menos efectos adversos en los derechos de la persona.

Como podemos apreciar, la evaluación de impacto del tratamiento de datos personales puede considerarse como "prospectiva", esto es, "se realizan al mismo tiempo que se diseña el programa y forman parte de la implementación del programa".[101] Se trata de una especie de test de daños, entendido como proceso de ponderación entre el beneficio generado por la operación de tratamiento de datos y el efecto negativo que esta misma pueda traer en los derechos de la persona del titular. Esta metodología no es ajena al estudio tradicional de la protección de datos, sino que más bien es una aplicación del principio de proporcionalidad.

Si bien no queda claro el resultado del proceso legislativo en Chile, en derecho comparado, el RGPD en el artículo 35 no prevé que deba usarse esta metodología en todos los tratamientos de datos personales, sino cuando "sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance contexto o fines entrañe un alto riesgo para los derechos y libertades de las personas físicas". Consecuentemente, prevé que debe realizarse la evaluación de impacto en las siguientes hipótesis:

a. Evaluación sistemática y exhaustiva de aspectos personales de personas físicas, que se base en un tratamiento automatizado como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar.

101 Banco Mundial/Banco Internacional de Reconstrucción y Fomento. *La evaluación de impacto en la práctica*. Documento elaborado por Paul Gertler, Sebastián Martínez, Patrick Premand, Laura B. Rawlings, Christel M.J. Vermeersh, 2011. ISBN 978-0-8213-8541-8; p. 31. Disponible en línea [consulta: 12.09.2021].

b. Tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10.

c. Observaciones sistemáticas a gran escala de una zona de acceso público.

Esta enumeración tiene un carácter meramente enunciativo, pudiendo la autoridad de control establecer y publicar listas de tratamiento de datos que requieran de evaluaciones de impacto, las cuales, en todo caso, deberán sujetarse a las reglas de coherencia previstas en los artículos 63 y siguientes del mismo Reglamento europeo.

5.4 Responsabilidad demostrada

Se trata de que los responsables del tratamiento de datos personales adopten medidas técnicas y organizativas que sean efectivas y verificables, encaminadas a asegurar el cumplimiento de los principios y normas de protección de datos.

Al respecto, se ha entendido que la responsabilidad demostrada responde a "un enfoque basado en el compromiso de la organización con incrementar sus estándares de protección para garantizarle a los ciudadanos un tratamiento idóneo de su información personal".[102] En este sentido, la OCDE señala al respecto: "Sobre todo controlador de datos [*responsable del tratamiento*] debe recaer la responsabilidad del cumplimiento de las medidas que hagan efectivos los principios señalados anteriormente".[103]

Consecuentemente, "los responsables del tratamiento de datos deben rendir cuentas del cumplimiento de las medidas que contemplan los demás principios de privacidad de la OCDE"[104], con independencia de la localización de los datos. Así, los procesos y sistemas deben generar evidencia sobre la aplicación efectiva de las reglas y principios de tratamiento de datos personales, a través de programas de gestión de riesgos, notificación de violaciones de seguridad que afecten a los datos personales, además de la posibilidad de adherira algún "código de conducta o acuerdo similar que dote de efecto vinculante a las Directrices", entre otras.

Como se puede apreciar, la responsabilidad demostrada representa en los hechos una inversión de la carga de la prueba, en el sentido que le corresponderá al responsable del tratamiento demostrar la debida diligencia en cada una de las fases del tratamiento de datos.

102 Superintendencia de Industria y Comercio, Colombia. "Guía para la implementación del principio de responsabilidad demostrada (*Accountability*)"; p. 4. Disponible en línea [consulta: 12.09.2021].

103 Organización para la Cooperación y el Desarrollo Económico (OCDE). "Directrices sobre la protección de la privacidad y los flujos transfronterizos de información" (2002). Disponible en línea [consulta: 12.09.2021].

104 OCDE-BID. "Políticas de banda ancha para América Latina y el Caribe. Un manual para la economía digital" (2016). Capítulo 15: Protección de la privacidad. Disponible en línea [consulta: 12.09.2021].

5.5 Enfoque de riesgos y gestión de seguridad de los datos personales

De acuerdo al Reglamento General de Protección de Datos (RGPD), las medidas técnicas y organizativas a que nos hemos referido deben tener en cuenta "la naturaleza, el ámbito, el contexto y los fines del tratamiento así como el riesgo para los derechos y libertades de las personas físicas".[105] Se trata de que los responsables del tratamiento adopten una actitud de vigilancia activa de los referidos riesgos.

Para ello, en primer lugar se deben identificar los riesgos y ponderarlos, para luego desarrollar planes de mitigación de los efectos adversos asociados a las amenazas identificadas. En esta labor, los encargados deben considerar los tipos de tratamiento de datos que efectúan, la naturaleza de los datos personales que son objeto de tratamiento, el número de personas afectadas por el tratamiento y la cantidad/variedad de tratamientos que una misma organización lleva a cabo.[106]

A vía ejemplar, se describen a continuación algunas de las medidas técnicas y organizativas que debieran adoptarse.

Medida	Riesgo que se busca gestionar
Seudonimización y el cifrado de datos personales	Filtraciones de datos.
Respaldos de bases de datos	La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida. en caso de incidente físico o técnico. permitirá enfrentar pérdidas, destrucciones y modificaciones indebidas de datos.
Gestión de riesgos	Los sistemas deben permitir hacer un monitoreo continuo de los riesgos operacionales. Identificar las brechas de seguridad permitirá implementar estrategias de seguridad proactivas y precaver quiebres de servicio, permitiendo la restauración eficiente de los datos y sistemas. Realizar simulaciones de seguridad y *hacking* ético permitirá identificar brechas y planificar el cierre de las detectadas.

105 Considerando 74 RGPD.
106 Agencia Española de Protección de Datos Personales. Guía del Reglamento General de Protección de Datos. Para responsables de tratamiento (Guía Protección de datos UE). Disponible en línea [consulta: 12.09.2021].

Gestión de incidentes de seguridad	La implementación de mecanismos de alerta, documentación y gestión de los incidentes permitirá mitigar los efectos del incidente y prevenir incidentes a futuro.
Notificar quiebres de seguridad	La notificación, tanto a la autoridad como al entorno (titulares de datos y cadenas de suministros y de relaciones institucionales), contribuye a la gestión de seguridad del entorno, precaviendo incidentes futuros además de mitigar los efectos en los derechos de las personas por el quiebre de seguridad. Cuando el quiebre de seguridad es producto de la comisión de un delito, implicará la persecución de la responsabilidad penal. En el caso de Chile, la Circular Nº 3633 de 24 de enero de 2018, de la Superintendencia de Bancos, recopilación actualizada de normas, capítulos 1-13 y 20-8, prevé que los bancos deben informar a la Superintendencia los incidentes operacionales relevantes y además establece las condiciones que se deben observar para generar y mantener una base de incidentes en el ámbito de la ciberseguridad. Este documento señala también que los bancos deben comunicar de inmediato los incidentes operacionales relevantes (aquellos que afecten la continuidad de negocios, seguridad de la información o la imagen de la institución). Lo que se debe informar es lo siguiente: – Nombre de la entidad informante. – Datos de la persona encargada de enviar la información: nombre, cargo, correo electrónico y teléfono celular. – Fecha y hora de inicio del evento. – Explicación del incidente: la situación que originó y su causa inmediata.

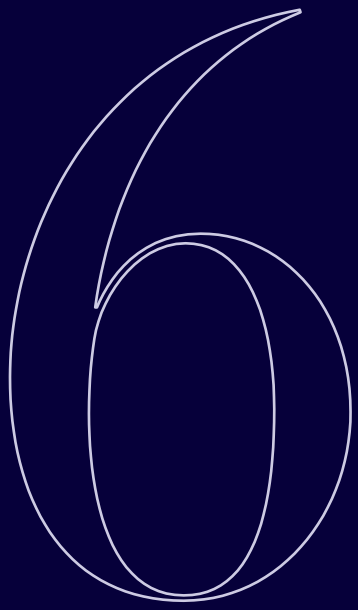
Adicionalmente, la notificación de los "quiebres de seguridad" o "violaciones de la seguridad de los datos personales" a los titulares de datos personales resulta un imperativo desde la protección de sus derechos. Estas comunicaciones deben contener al menos lo siguiente:

- Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive cuando sea posible, las categorías y el número aproximado de interesados afectados.
- Comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.
- Describir las posibles consecuencias de la violación de seguridad de los datos personales.

— Describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

La comunicación a los usuarios dice relación con que ellos son los dueños de los datos, pero además por la necesidad de que ellos mismos adopten las medidas que permitan mitigar los efectos del quiebre de seguridad, como por ejemplo eliminar o bloquear tarjetas de pago.

La comunicación debe ser en un lenguaje claro y sencillo, detallando la naturaleza de la violación de la seguridad de los datos personales; el nombre y los datos de contacto del encargado de seguridad y del punto de contacto en el que pueda obtenerse más información; las posibles consecuencias de la violación de seguridad de los datos personales; y las medidas adoptadas o propuestas incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.



Los derechos de los titulares de datos frente a la doctrina y jurisprudencia

← Índice de contenidos

Las diversas legislaciones en materia de protección de datos, incluida la chilena, por influjo de la estandarización normativa internacional han planteado que los titulares de datos o interesados tienen cuatro tipos de derechos diferentes, en lo que a sus datos personales concierne.

Se trata de los derechos de **acceso**, de **rectificación**, de **cancelación** (eliminación) y de **oposición**, los que por el acrónimo formado por sus iniciales son conocidos como **derechos ARCO**[107], y por expresa disposición legal no pueden ser limitados por medio de ningún acto o convención (art. 13 de la Ley Nº 19.628), por constituir precisamente el núcleo del derecho fundamental a la protección de datos.

6.1 Derecho de acceso

Se ha establecido como derecho primario en materia de protección de datos, lo que implica que el responsable del tratamiento de datos debe proporcionar, cuando así se le solicite, información relativa a los datos concretos de carácter personal que son objeto de tratamiento, así como al origen de los mismos, las finalidades de los correspondientes tratamientos y los destinatarios o categorías de destinatarios a quienes se comunica o pretende comunicar dichos datos.

Sin embargo, también pesa sobre ellos la obligación de que cualquier información que se proporcione al interesado deba facilitarse de forma inteligible, esto es, empleando para ello un lenguaje claro y sencillo.

107 En la legislación chilena están expresamente consagrados en los arts. 5° y 6° de la Ley N° 19.628 de 1999, con la particularidad de que no se habla del derecho de oposición, pero sí del bloqueo, entendiendo que procede cuando los datos son inexactos o incompletos: debe negarse la posibilidad de su consulta por terceros hasta obtener certeza respecto de los mismos.

A su vez, la Agencia Española de Protección de Datos ha sostenido que este derecho consiste en la facultad o capacidad que se reconoce al afectado de recabar información de sus datos de carácter personal incluidos y tratados en los sistemas automatizados.

El acceso podrá consistir en la mera consulta de los registros por medio de la visualización, o en la comunicación de los datos pertinentes por escrito, copia o telecopia, certificada o no; en cualquier caso, la información deberá ser legible e inteligible cualquiera sea el medio utilizado.

En nuestro país, el derecho de acceso está regulado en el artículo 12 de la Ley Nº 19.628, que establece que "toda persona tiene derecho a exigir a quien sea responsable de un banco, que se dedique en forma pública o privada al tratamiento de datos personales, información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente".

Adicionalmente, los interesados tienen la facultad de solicitar copia gratuita del registro que se tiene de ellos, pero solo pueden ejercer dicha facultad cuando hayan transcurrido a lo menos seis meses desde la anterior oportunidad en que hicieron uso de este derecho; aparentemente, el legislador quiso cautelar también los intereses de quienes realizan operaciones de tratamiento de datos, especialmente las oficinas de crédito, evitando que les pidieran documentación gratuita en forma permanente.

Es decir, se puede ejercer el derecho de acceso en cualquier momento, el cual bien puede satisfacerse por parte de los responsables de tratamiento de datos exhibiendo los datos en una pantalla, pero para solicitar copias gratuitas del registro deben haber transcurrido a lo menos 6 meses desde la última vez que se pidieron.

6.2 Derecho de rectificación

Se trata de un derecho emanado del principio de calidad que obliga al que realiza el tratamiento de datos personales a mantener estos tan completos y actualizados como se requiera conforme a los fines.

El derecho de rectificación es el que tiene el titular de los datos para solicitar, a la persona responsable, la rectificación o modificación de los datos de carácter personal que pudieran resultar incompletos o inexactos, es decir, se trata de un derecho emanado del principio de calidad que obliga al que realiza el tratamiento de datos personales a mantener estos tan completos y actualizados como se requiera conforme a los fines.

En nuestra legislación, este derecho se contempla en el artículo 12 inciso segundo de la Ley N° 19.628, estableciendo al respecto que "en caso de que los datos personales sean erróneos, inexactos, equívocos o incompletos, y así se acredite, tendrá derecho a que se modifiquen", sin perjuicio de otras regulaciones particulares que inciden en la materia, como la gratuidad de su ejercicio y el deber del responsable de comunicar esta rectificación a todos quienes se le haya entregado tales datos.

En resumidas cuentas, le asiste, al titular de los datos consignados en registros o bases de datos personales, el derecho de exigir al responsable del tratamiento la enmienda de aquellos datos que resulten inexactos o incompletos, y en todo caso, el responsable del tratamiento no puede exigir contraprestación alguna por hacer las rectificaciones de datos inexactos.

6.3 Derecho de cancelacióno supresión

El derecho de cancelación otorga la facultad de exigir la eliminación o supresión de los datos de carácter personal que pudieran resultar innecesarios o excesivos, o cuya tenencia carezca del consentimiento del interesado o del fundamento legal que justifique su utilización. No obstante, no procede la cancelación cuando los datos de carácter personal deban ser conservados para el cumplimiento de una obligación impuesta sobre la persona responsable del tratamiento, por la legislación o por las relaciones contractuales entre la persona responsable y el interesado, en su caso, o cuando existiera una obligación de conservar los datos.

Alguien no podría, por ejemplo, entregar sus datos personales a una casa comercial para obtener un crédito y luego ejercer el derecho de cancelación de los datos, mientras la relación contractual persiste con dicha casa.

Al igual que en el caso del derecho de rectificación, el responsable no podrá exigir contraprestación alguna cuando un titular lo ejerza; es más, la obligación de suprimir datos debe ejercerse por el responsable *motu proprio*, tan pronto como detecte que el almacenamiento de los mismos carece de fundamento legal o cuando estuvieren caducos en relación a la finalidad de los mismos, pues de lo contrario incurrirá en responsabilidad.

6.4 Derecho de oposición

Finalmente, el último de los derechos ARCO es el derecho de oposición, que habilita al titular de los datos a oponerse al tratamiento de datos de carácter personal cuando concurra una razón legítima derivada de su concreta situación personal, salvo en aquellos casos en los que el tratamiento sea necesario para el cumplimiento de una obligación legal impuesta sobre quien realiza el tratamiento de datos.

Para ilustrarlo con un ejemplo, imaginemos el caso de quien en Chile aparece como deudor en una entidad de información crediticia como el Boletín Comercial (llamado desde antiguo "el Peneca Verde") por el no pago de un pagaré, cuando en realidad en los tribunales se está discutiendo la falsificación del pagaré de referencia. Entonces, en el ejercicio de sus derechos, esa persona puede *oponerse* y exigir el retiro de la publicación, porque la información no reúne las necesarias condiciones de certeza, incumpliendo así el principio de calidad.

También está contemplado el ejercicio de este derecho para cualquier titular de datos que desee oponerse a decisiones automatizadas que conlleven efectos jurídicos, y basadas únicamente en un tratamiento automatizado de datos de carácter personal: un asunto de dignidad, si consideramos que es el juzgamiento de una persona por una máquina.

En Chile, el derecho de oposición está contemplado en el artículo 3º inciso segundo de la ley sobre protección de la vida privada, pero en términos ambiguos: "El titular puede oponerse a la utilización de sus datos personales con fines de publicidad, investigación de mercado o encuestas de opinión".

Así, es en la ley sobre acceso a la información pública (Ley Nº 20.285) donde este derecho encuentra mayor consistencia, pues su artículo 20 contempla que los organismos públicos, frente a una solicitud de entrega de información que puede afectar derechos de terceros, tienen la obligación de comunicárselo a esos terceros para el even-

tual ejercicio, por estos, de "la facultad que les asiste para oponerse a la entrega de los documentos solicitados", entre otras razones, por contener datos de carácter personal.

Existe también en nuestra llamada ley de protección de datos la figura del bloqueo de datos, que es una consecuencia del ejercicio del derecho de oposición y consiste en "la suspensión temporal de cualquier operación de tratamiento de los datos almacenados" (art. 2º, letra b), y opera respecto de los datos personales cuya exactitud no pueda ser establecida o cuya vigencia sea dudosa, y respecto de los cuales no corresponda la cancelación.

Retomando el ejemplo de más arriba, el Boletín Comercial puede, ante la impugnación de una información que no reúne los requisitos de calidad dada la falta de certeza (como la disputa judicial sobre la validez del pagaré), bloquear la información hasta que exista una sentencia a firme sobre el punto; no debería cancelarla, dado que su misión legal es, precisamente, dar cuenta de este tipo de asuntos.

6.5 Cambios en el ámbito de los derechos a partir de la entrada en vigencia del RGPD

El panorama internacional de los derechos de las personas en materia de protección de datos, que había sido estable en el tiempo, cambió el 25 de mayo de 2018 con la entrada en vigor del Reglamento General de Protección de Datos, pues este introdujo algunas innovaciones.

La primera de ellas es que el derecho de cancelación de datos, manteniendo su contenido, pasó a llamarse "**de supresión**", evitando así ciertas confusiones con la figura de la *cancelación*, propia del ámbito del derecho civil, que es la constancia que deja el acreedor en un determinado título de que la deuda ha sido pagada.[108]

Otra innovación fue la incorporación de un nuevo derecho de las personas, el derecho a la **portabilidad de los datos**, el cual faculta a las personas a exigir a quienes realizan operaciones de tratamiento de datos, que le entreguen sus datos personales en un formato estructurado y de uso común, o que los transmitan a otro responsable del tratamiento, bajo determinadas condiciones.[109]

Por supuesto que el Reglamento estableció también algunos otros derechos en favor de las personas, como el de la limitación del tratamiento en ciertas condiciones especiales, o que las personas no sean objeto de decisiones basadas en tratamientos automatizados[110], pero

108 Parece algo complejo, pero en realidad es sumamente simple y se da en el día a día de los pequeños comercios que venden "fiado": cuando al final del mes el cliente paga, el comerciante cancela, esto es, *tarja* o borra del listado de lo que se le debe lo que efectivamente le ha sido pagado.

109 Desde luego, el derecho a la portabilidad de los datos personales no ha sido incorporado a la legislación chilena, pero el Segundo Informe de la Comisión de Constitución, Legislación, Justicia y Reglamento del Senado, de 16 de marzo de 2020, recaído en el proyecto de ley que se recoge en los Boletines Nº 11.092-07 y Nº 11.144-07 (refundidos), establece el derecho a la portabilidad de los datos personales, por el cual el titular de datos tiene derecho a solicitar y recibir una copia de los datos personales que le conciernen y que haya facilitado al responsable, en un formato estructurado, genérico y de uso común, que permita ser operado por distintos sistemas, y a comunicarlos o transferirlos a otro responsable de datos, en determinados supuestos que el proyecto detalla.

110 "El RGPD amplía el catálogo de derechos que la Directiva 95/46/CE reconocía. Dicha ampliación es, por un lado, cuantitativa, puesto que se reconocen explícitamente nuevos derechos; por otro lado también es cualitativa, dado que se intentan adaptar a la realidad digital –con más o menos éxito– tanto los nuevos derechos como los que ya existían", afirma Adrian Di Pizzo Chiaccio en *La expansión del derecho al olvido*

los fundamentales son el de portabilidad, rectificación, oposición, supresión y el de acceso, que en adelante pasarán a ser conocidos por el acrónimo que forman sus primeras letras: **derechos PROSA**.

Ahora, más que memorizar siglas, lo importante es tener presente que estas definiciones, principios, derechos y deberes constituyen el núcleo esencial de los estándares internacionales de protección de datos, y la amplia generalidad de ellos están presentes en nuestra legislación nacional, por tanto, tienen la fuerza normativa y exigibilidad prevista para las leyes.

digital (Atelier, Barcelona, 2018); p. 267.

6.6 Aplicación del derecho de cancelacióna internet: el "derecho al olvido"

Si bien el derecho al olvido "ha ocupado una amplia literatura mediática y jurídica durante el último lustro acompañando la explosiva omnipresencia de Internet en nuestras vidas"[111], hasta el año 2009 ni siquiera las entidades europeas de protección de datos se habían ocupado de este asunto.

Incluso, el 1 de diciembre de ese año adoptaron un dictamen ampulosamente titulado "*The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*"[112], que nada dice del tema que ocuparía los mayores debates en los años siguientes.

Porque en 2010, Viviane Reding, quien ha sido Comisaria de Justicia, Derechos Fundamentales y Ciudadanía y también Comisaria de Información y Medios de la Comisión Europea, a estas alturas un icono de la lucha por el respeto del derecho a la protección de los datos personales, planteó que "los usuarios de Internet deben tener un control efectivo de los contenidos que ponen en línea y ser capaces de corregirlos, retirarlos o eliminarlos a voluntad. En la reciente consulta pública sobre la revisión de las normas de protección de datos, se nos dijo que debería existir 'un derecho a ser olvidado'. Necesitamos mirar más de cerca esa idea. Más control también significa poder mover sus datos de un lugar a otro, y tenerlos correctamente eliminados de la primera ubicación en el proceso"[113], destacando así tanto el olvido como la portabilidad de los datos, aunque con un enfoque algo más de negocios: lo que se quería o entendía era que los ciudadanos pudieran trasladar sus datos de una plataforma informá-

111 RALLO LOMBARTE, Artemi: *El derecho al olvido en internet. Google versus España*, Centro de Estudios Constitucionales, Madrid, 2014; p. 17.

112 Documento preparado por el Grupo de Trabajo del Artículo 29. Disponible en línea [consulta: 15.10.2020].

113 Discurso de Viviane Reding pronunciado en Bruselas, el 22 de junio de 2010, en la Cámara Norteamericana de Comercio ante la Unión Europea. Disponible en línea (solo inglés) [consulta: 15.10.2020].

tica a otra y que ello implicara el borrado definitivo de los datos de la plataforma cedente. Es decir, se asoció primero, erróneamente, olvido con portabilidad, pero prontamente tomaron derroteros distintos.

Recién el 4 de noviembre de 2010, por primera vez en un documento oficial, como fue una Comunicación de la Comisión Europea[114], se menciona explícitamente el **derecho al olvido** como parte integrante del reforzamiento de los derechos de las personas y el control efectivo sobre sus propios datos, cuestión crítica en relación a las malas prácticas de las plataformas de redes sociales en que, en los hechos y una vez aceptados los términos y condiciones, la voluntad de los usuarios devenía en irrelevante.

Dicha Comunicación postula que se debe estudiar y clarificar "el derecho a ser olvidado", que ya entiende como "el derecho de las personas a que sus datos no se traten y se supriman cuando dejan de ser necesarios con fines legítimos".

En este estado de cosas, el 25 de enero de 2012 se comenzó a discutir una reforma mayor en materia de protección de datos personales, cual es el Reglamento General de Protección de Datos, que a esas alturas del debate consideraba el derecho al olvido como una poco gloriosa comunicación que debían hacer los responsables a terceros sobre las solicitudes de cancelación de datos personales que recibieron, para efectos de actualizar las bases de datos.

Mientras se debatían estos aspectos, y las negociaciones del nuevo Reglamento se entrampaban bajo el *lobby* de las empresas tecnológicas, algo extraordinario sucedió y los hechos serán aquí relatados en base a las explicaciones de Alejandro Touriño.[115]

114 Nos referimos a la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones titulada "Un enfoque global de la protección de los datos personales en la Unión Europea". Disponible en línea [consulta: 15.10.2020].

115 TOURIÑO, Alejandro: *El derecho al olvido y a la intimidad en internet,* Los Libros de la Catarata, Madrid, 2014; pp. 34-41.

Ocurrió que el diario español *La Vanguardia* había publicado, a principios de 1998, en su edición en papel y luego en su edición digital, dos avisos relativos a la subasta de inmuebles embargados al abogado Mario Costeja González por deudas a la Seguridad Social.

Mucho tiempo después, en noviembre de 2009, el propio Costeja se dio cuenta de que, cuando introducía su nombre y apellidos en el buscador web de Google, aparecían todavía esos anuncios y, para peor en el caso de alguien que vive de su prestigio, asociados a su nombre.

Costeja se puso entonces en contacto con el diario para pedir la bajada de los contenidos, argumentando tanto que la situación del embargo se había solucionado hace muchos años atrás, como también que para entonces no era relevante de forma alguna, sino que solo causaba males innecesarios.

El diario *La Vanguardia* le contestó que no procedía cancelar o suprimir esos datos, pues los hechos habían sido veraces y que quien había solicitado la publicación había sido el propio Ministerio del Trabajo y de Asuntos Sociales, por lo que nada justificaba su retirada, máxime cuando lo que estaba en juego era el derecho a informar.

Mario Costeja intentó otra vía de solución en febrero de 2010, como fue solicitarle a la filial de Google en España (Google Spain S.L.) que ya no apareciera su nombre ligado a estos avisos, pero esta empresa le señaló que ella no era la indicada para resolver el problema, pues su giro se limitaba a la venta de publicidad sobre los resultados de las búsquedas, agregando que debía dirigirse a quien gestionaba el servicio de motor de búsqueda en internet (el servicio se llama Google Search): la empresa matriz Google Inc., con domicilio social en California, Estados Unidos de América, al otro lado del Atlántico.

Ante la imposibilidad de resolver el asunto en términos razonables, Costeja solicita la tutela de la Agencia Española de Protección de Datos para que *La Vanguardia* eliminase o modificase la publicación en lo concerniente a sus datos personales, o bien utilizare herramientas de exclusión de contenidos o, subsidiariamente, que se exigiese a Google Spain S.L. o Google Inc. eliminar dichos datos para que no fueran incluidos en sus resultados de búsqueda.

Sin embargo, la autoridad española de protección de datos solo dio lugar a la solicitud en lo referente a Google, tanto la matriz como la filial, instando a que ambas adoptaran las medidas necesarias para retirar los datos de su índice e imposibilitar el acceso futuro a los mismos, en consideración a que quienes gestionan motores de búsqueda están sometidos a la normativa de protección de datos.

Lo anterior, porque dichas empresas llevan a cabo operaciones de tratamiento de datos de las que son responsables y, por ende, los titulares de datos podían dirigirse directamente a los responsables de los motores de búsqueda solicitando suprimir los datos que les concernían, aun cuando la información de la página que pretenden *desindexar* del buscador esté justificada por ley.

Respecto al diario *La Vanguardia*, la Agencia española entendía que tenía justificación legal para actuar como lo hacía, pues actuaba por orden de una autoridad pública a efectos de darle la máxima publicidad posible a una subasta y conseguir la concurrencia de postores, no haciendo la señalada autoridad mayor cuestión de ello.[116]

La empresa Google no se conformó con dicha resolución administrativa y recurrió a la Audiencia Nacional[117] con dos recursos independientes (luego acumulados), solicitando la nulidad de la resolución de la Agencia Española de Protección de Datos, pero la Audiencia Nacional hizo uso de lo que Touriño graciosamente llama "el comodín de la llamada" (referencia a un popular programa concurso televisivo). Se refiere a una atribución, en materia de cuestiones prejudiciales de derecho comunitario europeo, que habilita a los tribunales de los Estados de la Unión Europea a suspender el

116 Este razonamiento está contenido en la Resolución R/01680/2010, de 30 de julio de 2010, recaída en el Procedimiento TD/00650/2010.

117 La Audiencia Nacional es un órgano jurisdiccional con competencia en todo el territorio español, constituyendo un tribunal centralizado y especializado para el conocimiento de determinadas materias que vienen atribuidas por ley; se ocupa de los delitos de mayor gravedad y relevancia social como son, entre otros, los de terrorismo, crimen organizado, narcotráfico, delitos contra la Corona y los delitos económicos que causan grave perjuicio a la economía nacional. En materia contencioso-administrativa, la Audiencia Nacional fiscaliza las resoluciones de la Administración del Estado y es por eso que Google recurre a ella para anular la resolución de la Agencia Española de Protección de Datos.

procedimiento a efectos de consultarle al Tribunal de Justicia de la Unión Europea (en adelante TJUE) acerca de la interpretación de asuntos de derecho comunitario.

La Audiencia Nacional consultó sobre una serie de cuestiones[118] que el TJUE integró en tres preguntas: a) si el derecho europeo en materia de protección de datos se aplica a los buscadores de internet operados desde fuera de la Unión Europea; b) si la actividad del motor de búsqueda de Google encaja en el concepto de tratamiento de datos contenido en el artículo 2 de la Directiva 95/46/CE –"cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción"– y finalmente, c) si los derechos de supresión y bloqueo de datos incluyen la facultad de dirigirse a los buscadores para impedir la indexación de la información referida a una persona, así como acerca de las competencias de las agencias nacionales de protección de datos al respecto.

Hacemos notar aquí que se trata de una consulta, por lo que no es que el TJUE resuelva el fondo del asunto aunque, indudablemente, es difícil imaginar un fallo de un tribunal nacional que vaya en un sentido distinto del indicado por un tribunal de mayor jerarquía, al cual precisamente le ha consultado voluntariamente para esclarecer los nudos gordianos de la discusión, y más todavía cuando, según nos hacen presente Córdoba y Díez-Picazo, "la primacía del Derecho comunitario no solo comprende la de las normas positivas que lo integran, sino también, como es lógico, la interpretación que de las mismas haga el único Tribunal con competencia para ello".[119]

118 El texto de lo consultado por la Audiencia Nacional está disponible en línea [consulta: 15.10.2020].

119 Córdoba Castroverde, Diego y Díez-Picazo Giménez, Ignacio: "Reflexiones sobre los retos de la protección de la privacidad en un entorno tecnológico". En *El derecho a la privacidad en un nuevo entorno tecnológico*, VV.AA., Centro de Estudios Políticos y Constitucionales, Madrid, 2016; p. 115.

El 13 de mayo de 2014, la Gran Sala del Tribunal de Justicia de la Unión Europea resuelve el procedimiento entre Google Spain S.L., Google Inc. y Agencia Española de Protección de Datos (AEPD), Mario Costeja González (asunto C-131/12), recordando que ya en otro caso había declarado que la conducta que consiste en hacer referencia en una página web a datos personales, debe considerarse tratamiento de datos personales.[120]

Por consiguiente, cuando Google Search explora internet de manera automatizada, constante y sistemática en busca de la información que allí se publica, y en su búsqueda recoge datos que extrae, registra, organiza y posteriormente indexa, conservando esa información en sus servidores y luego comunicando y facilitando el acceso a los resultados a sus usuarios, presentándolos en forma de listados de resultados de sus búsquedas, entonces dicha actividad debe calificarse de "tratamiento" en el sentido de la Directiva 95/46/CE[121], sin que sea relevante que el gestor del motor de búsqueda también realice las mismas operaciones con otros tipos de información diferentes a datos personales, o que no distinga entre estos y los datos personales.

Y como es el gestor del motor de búsqueda quien determina los fines y los medios de esta actividad y, en definitiva, el tratamiento de datos personales que efectúa él mismo en el marco de esta, la conclusión es que debe considerársele "responsable" de dicho tratamiento, conforme a la Directiva, pues lo contrario sería hacer ilusorio el rol de la normativa en cuanto a garantizar una protección eficaz y completa de los derechos de los titulares de los datos (los "interesados"); y ello es precisamente lo que ocurriría si se les excluyera de la aplicación de la Directiva, porque estos sencillamente optan por no ejercer control sobre los datos personales que tratan, lo que en definitiva sería desconocer que la "actividad de los motores de búsqueda des-

120 Se refiere a la decisión del TJUE recaída en el caso Lindqvist, asunto C-101/01, en cuyo parágrafo 25 plantea que "la conducta que consiste en hacer referencia, en una página web, a datos personales debe considerarse un tratamiento de esta índole», esto es, tratamiento de datos personales.

121 Recordemos que tratamiento de datos personales es, para la Directiva 95/46/CE "cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción".

empeña un papel decisivo en la difusión global de dichos datos en la medida que facilita su acceso a todo internauta que lleva a cabo una búsqueda a partir del nombre".

Son precisamente estas búsquedas de los usuarios, que se llevan a cabo partir del nombre de una persona física, las que permiten obtener mediante una lista de resultados una visión estructurada de la información relativa a la persona buscada, estableciendo un perfil más o menos detallado de la misma, lo que abre la puerta a la afectación significativa de los derechos fundamentales de respeto de la vida privada y de protección de datos personales, por lo que para el TJUE es claro que el gestor de este motor, como entidad que determina los fines y los medios más efectivos de llevar a cabo su labor, debe garantizar en el marco de sus responsabilidades, competencias y posibilidades que dicha actividad satisface las exigencias de la Directiva 95/46/CE; es decir, el tribunal "ha negado que el automatismo de los buscadores los convierta en intermediarios neutrales ajenos a las obligaciones derivadas del tratamiento de datos"[122], pues son ellos los que definen la organización, estructura y presentación de la información.

Determinado el punto de que los gestores de motores de búsqueda en internet sí realizan operaciones de tratamiento de datos personales, lo que los sitúa dentro de la esfera normativa de la Directiva 95/46/CE, el TJUE se lanza a determinar si existen elementos que le den competencia a entidades administrativas y jurisdiccionales de la Unión Europea respecto de motores de búsqueda que operan desde fuera de ella.

Al respecto, razona que el servicio Google Search indexa páginas web de todo el mundo, incluyendo las páginas web ubicadas en España, no solo para facilitar el acceso a los contenidos, sino que aprovecha esta actividad para incluir publicidad asociada a los patrones de búsqueda

122 RALLO LOMBARTE, Artemi: "El debate europeo sobre el derecho al olvido en internet". En *Hacia un Nuevo Derecho Europeo de Protección de Datos*, editado por Rallo Lombarte y Rosario García Mahamut, Tirant lo Blanch, Valencia, 2015; p. 735.

introducidos por los internautas del país; para capitalizar lo anterior, utiliza una empresa filial llamada Google Spain S.L. que actúa como agente comercial del grupo ante España, Estado miembro de la Unión.

Dado lo anterior, el tribunal considera que este es propiamente un establecimiento que está involucrado en la actividad de promoción y venta de espacios publicitarios, constituyendo la labor de Google Spain S.L. parte esencial de la actividad comercial del grupo Google en España y está indisolublemente ligado al servicio Google Search, lo que vincula al grupo Google con el territorio de un Estado miembro de la Unión Europea, y lo hace a través del ejercicio efectivo y real de una actividad publicitaria y comercial mediante una instalación estable.

La forma jurídica que adopte el grupo Google en un país concreto, sea una simple sucursal o una filial con personalidad jurídica propia, no es un factor determinante a estos efectos, sino que lo importante analizar el conjunto de actividades que lleva adelante[123]; este asunto no puede interpretarse en forma restrictiva, pues lo que se requiere es garantizar una protección eficaz y completa de las libertades y derechos fundamentales de las personas, siendo evidente que "las actividades del gestor del motor de búsqueda y las de su establecimiento situado en el Estado miembro de que se trate están indisociablemente ligadas, dado que las actividades relativas a los espacios publicitarios constituyen el medio para que el motor de búsqueda en cuestión sea económicamente rentable y dado que este motor es, al mismo tiempo, el medio que permite realizar las mencionadas actividades" (parágrafo 56 de la sentencia).

Todo lo anterior lleva al TJUE a la convicción de que el tratamiento de datos personales controvertidos se lleva a cabo en el marco de la actividad publicitaria y comercial del establecimiento del responsable del tratamiento en territorio de un Estado miembro de la Unión Europea, en el caso de autos el territorio español, pues el gestor del

123 Cabe hacer presente que, con esta lógica comercial, también existe Google Chile, con oficinas en Santiago de Chile y que actúa con la misma lógica de Google Spain, por lo que también es una filial de Google Inc. Pero va más allá todavía: en nuestro país se encuentra el primer centro de datos del hemisferio sur del grupo Google, es decir que en Chile, directamente, se realizan operaciones de tratamiento de datos sujetas a la Ley N° 19.628.

motor de búsqueda ha creado una sucursal o filial destinada a garantizar la promoción y la venta de espacios publicitarios propuestos por el mencionado motor y cuya actividad se dirige a los habitantes de ese país.

Por último, la sentencia del TJUE discurre sobre la pregunta de si el gestor de un motor de búsqueda está obligado a eliminar de la lista de resultados, obtenida tras una búsqueda efectuada a partir del nombre de una persona, vínculos a páginas web publicadas por terceros y que contienen información relativa a determinada persona, aun cuando la publicación de dichas páginas sea lícita.

Afirma el tribunal en el parágrafo 66 que la normativa de protección de datos personales vigente a la época, en particular la Directiva 95/46/CE, "tiene por objeto garantizar un nivel elevado de protección de las libertades y los derechos fundamentales de las personas físicas, sobre todo de su vida privada, en relación con el tratamiento de datos personales".

Y en ese marco, sostiene el TJUE que incumbe al responsable del tratamiento garantizar que los datos personales sean tratados de manera leal, lícita y recogidos con fines determinados explícitos y legítimos, que no sean procesados posteriormente de manera incompatible con dichos fines, que reúnan las características de adecuados pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente; que además sean exactos y cuando es necesario, actualizados y, por último, que se conserven de la forma que permita la identificación de los titulares durante un periodo no superior al indispensable para cumplir los fines para los que fueron recogidos o para los que se traten ulteriormente; en este contexto "el mencionado responsable debe adoptar todas las medidas razonables para que los datos que no responden a los requisitos de esta disposición sean suprimidos o rectificados".

En consecuencia, el titular o interesado puede dirigir las solicitudes de rectificación, supresión, bloqueo y oposición, de acuerdo al parágrafo 77,"directamente al responsable del tratamiento que debe entonces examinar debidamente su fundamento y, en su caso, poner fin al tratamiento de los datos controvertidos. Cuando el responsable del

tratamiento no accede a las solicitudes, el interesado puede acudir a la autoridad de control o a los tribunales para que estos lleven a cabo las comprobaciones necesarias y ordenen a dicho gestor las medidas precisas en consecuencia".

Reitera el tribunal, en el parágrafo 80, que:

> "Un tratamiento de datos personales como el controvertido en el litigio principal, efectuado por el gestor de un motor de búsqueda, puede afectar significativamente a los derechos fundamentales de respeto de la vida privada y de protección de datos personales cuando la búsqueda realizada sirviéndose de ese motor de búsqueda se lleva a cabo a partir del nombre de una persona física, toda vez que dicho tratamiento permite a cualquier internauta obtener mediante la lista de resultados una visión estructurada de la información relativa a esta persona que puede hallarse en Internet, que afecta potencialmente a una multitud de aspectos de su vida privada, que, sin dicho motor, no se habrían interconectado o solo podrían haberlo sido muy difícilmente y que le permite de este modo establecer un perfil más o menos detallado de la persona de que se trate".

Además, agrega que "el efecto de la injerencia en dichos derechos del interesado se multiplica debido al importante papel que desempeñan Internet y los motores de búsqueda en la sociedad moderna, que confieren a la información contenida en tal lista de resultados carácter ubicuo", por lo que, vista la gravedad potencial de esta injerencia, es obligado para el tribunal "declarar que el mero interés económico del gestor de tal motor en este tratamiento no la justifica" y, por ende, "la autoridad de control o el órgano jurisdiccional pueden ordenar a dicho gestor eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona vínculos a páginas web, publicadas por terceros y que contienen información relativas a esta persona", sin que una orden en dicho sentido presuponga también una orden de carácter previo o simultáneo para la página web que los contenidos han sido publicados.

Ello en razón de que la información publicada en un sitio de internet puede ser copiada en otros sitios y de que los responsables de su publicación no están siempre sujetos al derecho de la Unión Europea o que puede tratarse de información con fines exclusivamente periodísticos y beneficiarse de las excepciones correspondientes, que no es el caso del tratamiento que lleva a cabo el gestor de un motor de búsqueda, pues una protección eficaz y completa de los interesados o titulares de los datos no podría alcanzarse si tuvieran que obtener, con carácter previo o en paralelo, la eliminación de la información por parte de los autores o editores de la misma.

Concluye entonces, el tribunal, que la Directiva 95/46/CE debe interpretarse en el sentido de que para respetar los derechos que establecen estas disposiciones, el gestor de un motor de búsqueda puede verse obligado a eliminar de la lista de resultados obtenidos tras una búsqueda efectuada a partir del nombre de una persona, los vínculos a páginas web publicadas por terceros, aunque la publicación de dichas páginas sea en sí misma lícita.

Precisa el TJUE que un tratamiento inicialmente lícito de datos exactos *puede devenir con el tiempo* en incompatible con la normativa de protección de datos, cuando los datos personales ya no sean necesarios en relación con los fines para los que se recogieron o trataron. Ello ocurre cuando son inadecuados, no pertinentes o excesivos en relación con estos fines y el tiempo transcurrido, por lo que deben eliminarse.

Entonces, el interesado puede solicitar que la información de que se trate ya no se ponga a disposición del público en general mediante su inclusión en la lista de resultados, dado que sus derechos prevalecen, en principio, no solo sobre el interés económico del gestor del motor de búsqueda, sino también sobre el interés de dicho público en encontrar la mencionada información; no es un derecho absoluto, sino que, por razones que deben apreciarse en concreto, como sería si el titular de los datos desempeñara un rol relevante en la vida pública, podría ser que la injerencia en sus derechos fundamentales esté justificada por el interés preponderante de dicho público en tener acceso la información que se trate.

Corral Talciani, comentando esta sentencia, propone también otros criterios razonablemente atendibles en que normalmente el derecho a la cancelación o supresión de datos personales no debería prevalecer, como son aquellos referidos a autoridades públicas o los de quienes opten a cargos de representación popular; los referidos a crímenes de lesa humanidad; aquellos que cometen ciertos delitos que "pueden representar un peligro para ciertos ambientes" (sospechamos que con esa ambigüedad se refiere a los depredadores sexuales de menores de edad), y cuando los hechos tienen relevancia para mantener la memoria histórica de una comunidad.[124]

Pero hay dos cuestiones que hay que tener muy claras: la primera es que la sentencia "no hace sino poner de manifiesto que los principios que configuran el derecho a la protección de datos, tal y como es concebido en el ámbito de la Unión Europea, son perfectamente aplicables a los tratamientos de datos personales llevados a cabo en el marco de los servicios de la Sociedad de la información", es decir, no se ha reinventado ningún derecho, bastando los propios de la protección de datos; la segunda es que **la sentencia nunca habla de un derecho al olvido**, salvo cuando menciona las alegaciones de las partes y el contenido del auto de planteamiento, según observa agudamente Puente Escobar.[125]

Esta decisión del TJUE generó un gran revuelo mediático que se extiende hasta nuestros días, y unidas a las revelaciones que realizara Edward Snowden en junio de 2013[126] sobre la existencia de "una sofisticada maquinaria de recolecta y análisis de datos referidos a

124 CORRAL TALCIANI, Hernán: "El derecho al olvido en internet: antecedentes y bases para su configuración jurídica". En *Revista Jurídica Digital UANDES* N° 1, Facultad de Derecho de la Universidad de los Andes, Santiago de Chile, 2017; p. 62. Disponible en línea [consulta: 15.10.2020].

125 PUENTE ESCOBAR, Agustín: "El 'derecho al olvido'". En *El Derecho de Internet*, coordinado por Francisco Pérez Bes, Atelier, Barcelona, 2016; pp. 182-183.

126 Como se recordará, Edward Snowden era un consultor tecnológico estadounidense, antiguo empleado de la Agencia Central de Inteligencia (CIA) y de la Agencia de Seguridad Nacional (NSA), que en junio del 2013 hizo públicos, a través de los periódicos *The Guardian* (Reino Unido) y *The Washington Post* (Estados Unidos), documentos secretos sobre la existencia de varios proyectos en curso de vigilancia masiva en las redes de comunicaciones electrónicas por parte de algunos gobiernos, en concomitancia con emblemáticas empresas del sector tecnológico (Microsoft, Google, Apple, Facebook, Yahoo!, Vodafone, British Telecommunications y otras), lo que hacían tanto a través de interceptores en las redes de fibra óptica, usando sistemas informáticos como Xkeyscore, Upstream, Dishfire y otros, como también a través de la incautación masiva de datos para su posterior análisis a través de programas como PRISM.

las comunicaciones, de alcance global, que se despliega a través de diferentes vías y programas y que deja manifiestamente obsoletas y carentes de sentido las proclamaciones, cautelas y garantías con las que los textos constitucionales y los instrumentos internacionales de reconocimiento de derechos intentan hacer valer el derecho a la vida privada y las salvaguardas conexas"[127], transformaron sustancialmente el panorama de la discusión político-legislativa del que sería el Reglamento General de Protección de Datos de la Unión Europea, de forma tal que este último, en vez de ser un genérico y anodino manual de buenas maneras, se transformó en una potenciada herramienta de protección de derechos fundamentales, en particular, el derecho a la protección de datos personales.[128]

Jurídicamente, la sentencia del TJUE, según sostienen Córdoba y Díez-Picazo, "implica el reconocimiento claro y explícito del 'derecho al olvido', cuya esencia radica en la supresión de datos e informaciones que con el transcurso del tiempo han perdido la razón de ser que las justificaron en su momento y el afectado desea que no sean del conocimiento público"[129], pero no solo es eso, sino que los alcances se extienden bastante más allá pues, siguiendo a los mismos autores, la protección de datos cambia radicalmente: a partir de la sentencia, es claro que, en primer lugar, "no es requisito del derecho al olvido que la información suministrada cause un perjuicio al interesado"; y, en segundo lugar, que la protección no dice relación con la eventual ilicitud de la información objeto de tratamiento, sino que opera

127 REVENGA SÁNCHEZ, Miguel: "El derecho a la intimidad: un derecho en demolición (y necesitado de reconstrucción)". En *El derecho a la privacidad en un nuevo entorno tecnológico*, VV.AA., Centro de Estudios Políticos y Constitucionales, Madrid, 2016; pp. 86-87.

128 La epopeya de lo que fue sacar adelante el proyecto de Reglamento puede visualizarse en la película documental franco-alemana de 2015 llamada *Democracy: Im rausch der daten*, del director David Bernet, que sigue el camino del eurodiputado verde Jan Philipp Albrecht, quien lucha, con todas las probabilidades en contra, por aprobar en el Parlamento Europeo una propuesta de consenso que tiene que pasar por sobre las más de 4.000 enmiendas presentadas para anular los efectos del Reglamento o paralizarlo, contando básicamente solo con la comisionada europea Viviane Reding como aliada.

129 CÓRDOBA CASTROVERDE, Diego y DÍEZ-PICAZO GIMÉNEZ, Ignacio: "Reflexiones sobre los retos de la protección de la privacidad en un entorno tecnológico". En *El Derecho a la Privacidad en un Nuevo Entorno Tecnológico*, VV.AA., Centro de Estudios Políticos y Constitucionales, Madrid, 2016; pp. 113-114. Entendemos que lo "claro y explícito" está referido a los alcances del derecho de supresión de datos personales y no a que el tribunal haya expresado que existía un *derecho al olvido*, pues ello no ocurrió.

también "frente a datos exactos cuyo conocimiento, por el tiempo transcurrido, ya no sean necesarios en relación con los fines para los que se recogieron o trataron".

En el caso concreto de Costeja González, ¿para qué se publicaron los datos en *La Vanguardia*? Para obtener postores en un remate de inmuebles. ¿Cuándo fue o debió tener lugar el señalado remate? Dieciséis años atrás. Entonces, ¿qué finalidad se cumple con mantener esa información publicada?

Y en tercer lugar, la protección puede perfectamente ser asimétrica, "en razón a los derechos invocables y los intereses que protegen los diferentes operadores de internet"[130]; es decir, no es forzoso obtener la "bajada" de los contenidos por parte del autor o editor de los mismos en forma previa a solicitar tal cosa al gestor del motor de búsqueda o viceversa, sino que perfectamente se puede dirigir esas pretensiones hacia uno u otro, e incluso la sentencia plantea en el parágrafo 87 que puede ser preferible dirigirse al motor de búsqueda en los casos en que él "puede constituir una injerencia mayor en el derecho fundamental al respeto de la vida privada del interesado que la publicación por el editor de esta página web".

Entonces, la idea de un "derecho al olvido" pasó finalmente de ser una especie de comunicación o aviso entre responsables de tratamiento, de que alguien había solicitado la supresión de sus datos personales, a ser un derecho reconocido expresamente en el Reglamento, con una dimensión y alcances muy distintos y saltando por sobre "el riesgo de que el derecho al olvido pudiera convertirse en una modalidad de censura", tal como preconizaban los "evangelistas de la libertad en la Red entremezclados con los intereses económicos de las poderosas multinacionales que operan en ella", los que habían

130 Ídem; p. 114.

provocado resultados efectivos en el entorpecimiento del proceso de discusión, enarbolando incluso el olvido como amenaza a la libertad de expresión y a la libertad de prensa, según hace presente Rallo.[131]

Pauner complementa lo anterior afirmando que "estas acusaciones desenfocan la causa legitimadora de la libertad de expresión que protege la difusión y recepción de información de todo asunto de interés público, pero no la publicación indiscriminada de cualquier tipo de dato personal irrelevante, caduco o cuya utilización ya no responde a la finalidad para la que fue recabado".[132]

Finalmente, lo que el Reglamento dice es: "Artículo 17. Derecho de supresión ('el derecho al olvido'). 1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando (…)" ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados, o si el interesado retira el consentimiento, o si se opone y no prevalezcan otros motivos legítimos para el tratamiento, o si los datos se han tratado ilícitamente, o sean necesarios para el cumplimiento de una obligación legal, o cuando se hayan obtenido para la oferta de servicios de la sociedad de la información y ya no se desee recibirlas.

El mismo artículo del Reglamento contempla excepciones al derecho de supresión de datos: no procede la supresión o cancelación si el tratamiento es necesario para ejercer el derecho a la libertad de expresión e información, o si es necesario para el cumplimiento de una obligación legal que requiera el tratamiento de datos, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, o por

131 RALLO LOMBARTE, Artemi: "El debate europeo sobre el derecho al olvido en internet". En *Hacia un nuevo derecho europeo de protección de datos*, editado por Rallo y Rosario García Mahamut, Tirant lo Blanch, Valencia, 2015; pp. 728–729.

132 PAUNER CHULVI, Cristina: "Implicancias del futuro reglamento europeo sobre protección de datos". En *Los derechos a la intimidad y a la privacidad en el siglo XXI*, coordinado por Antonio Fayos Gardó, Dykinson, Madrid, 2014; pp. 194-195.

El derecho al olvido, en la concepción del Reglamento General de Protección de Datos, es el derecho a exigir al responsable del tratamiento de datos que estos sean suprimidos o cancelados sin dilación cuando se cumplen ciertos requisitos, como el no ser necesarios en relación con la finalidad para los que fueron recogidos o tratados.

razones de la salud pública, o con fines de archivo, o con fines de investigación científica o histórica o fines estadísticos y también para la formulación de reclamaciones.

En síntesis, y en la parte que nos interesa, pues serán aspectos sobre los que volveremos, lo que debe tenerse presente es que el derecho al olvido, en la concepción del Reglamento General de Protección de Datos, es el derecho a exigir al responsable del tratamiento de datos que estos sean suprimidos o cancelados sin dilación cuando se cumplen ciertos requisitos, como el no ser necesarios en relación con la finalidad para los que fueron recogidos o tratados; pero también están previstas excepciones, como es el caso en que el tratamiento de los datos es necesario para ejercer el derecho a la libertad de expresión e información.

O como dice Muñoz Massouh, "una de las finalidades del derecho al olvido consiste en que lograr que se elimine de la red la información que haya sido publicada sin el consentimiento de su titular, garantizándose, de esa manera, que éste retome el control de aquella, o bien, porque aún difundida con su anuencia ha trascurrido cierto plazo desde su publicación original, el que hace razonable su cancelación o eliminación".[133]

Ahora bien, "el derecho al olvido no es el producto del mero capricho de algunos que su pasado no sea conocido, como afirman los críticos, sino que responde a una necesidad sentida por los ciudadanos de poder controlar la trazabilidad de su vida digital y poder eliminar, o limitar la difusión, de aquellos trazos cuya accesibilidad permanentepuede incidir negativamente en su carrera laboral, su crédito o sus relaciones sociales".[134]

133 MUÑOZ MASSOUH, Ana María: "Eliminación de datos personales en internet: el reconocimiento del derecho al olvido". En *Revista Chilena de Derecho y Tecnología* Vol. 4 N° 2, Facultad de Derecho de la Universidad de Chile, Santiago de Chile, 2015; p. 224. Disponible en línea [consulta: 15.10.2020].

134 MIERES MIERES, Luis Javier: *El derecho al olvido digital*, Fundación Alternativas, Madrid, 2014; p. 51.

Nótese que el derecho al olvido en el Reglamento no se menciona directamente, sino que aparece bajo una fórmula bastante extraña: "Derecho de supresión ('el derecho al olvido')". ¿Por qué esta singularidad?

Hay dos razones fundamentales para ello. La primera es que el "derecho al olvido" no es una categoría jurídica, no es un derecho propiamente tal[135], sino que es la denominación *con nombre de bolero*[136] con la que se conoce el concepto entre el público usuario de internet.

Y también aparece de esa forma, pues en realidad tampoco se trata de un derecho nuevo o distinto del derecho de cancelación o supresión, sino que solo se usa esa denominación cuando el derecho de cancelación se aplica a contenidos publicados en internet, tal como lo entiende Davara Fernández de Marcos, quien lo conceptualiza como "el derecho que tiene una persona física a exigir que se borren de manera definitiva sus datos personales y su rastro en la Red –haciéndolo inaccesible en el entorno online–, siempre que se cumplan unas determinadas circunstancias".[137]

Ello no es solo una interpretación doctrinaria, de hecho el Tribunal Constitucional de España ha sido más explícito todavía: "En suma, en el Reglamento se viene a legislar de forma más clara el derecho a la supresión de los datos personales de una determinada base que los contuviera. Eso, y no otra cosa, es el derecho al olvido"[138].

135 Por tanto, como realmente no existe un derecho subjetivo llamado "derecho al olvido", está fuera de todo lugar la *falacia del hombre de paja*, argumento revestido de lógica jurídica formulado por Pazos Castro, en el sentido de que si existe un derecho al olvido también existiría la obligación de olvidar exigible a todos: "La expresión 'derecho al olvido' evoca un imposible, ya que, en la medida en que todo derecho comporta una correlativa obligación, el derecho al olvido sencillamente no puede existir. ¿Puede una persona olvidar algo de forma voluntaria y automática? ¿Puede un órgano judicial adoptar una medida concreta para dar cumplimiento a la obligación de olvidar?"; véase al respecto Pazos Castro, Ricardo: "El mal llamado 'derecho al olvido' en la era de internet", en *Boletín del Ministerio de Justicia* Nº 2183, Madrid, 2015; p. 2015. Este argumento es muy repetido en Chile por grupos de interés y ONG detractoras de las implicancias del derecho de cancelación de datos para el buscador Google.

136 No es una originalidad esta denominación, sino que fue el primer Director de la Agencia Española de Protección de Datos, Juan José Martín-Casallo López, quien intervino el 28 de enero de 2013 en la Jornada "20 años de Protección de Datos en España" señalando que el nombre *derecho al olvido* le sonaba a "bolero sudamericano".

137 DAVARA FERNÁNDEZ DE MARCOS, Elena: "El Reglamento Europeo de Protección de Datos". En *Derecho digital. Perspectiva interdisciplinar*, obra en colaboración dirigida por Víctor Cazurro Barahona, J.M. Bosch Editor, Barcelona, 2017; p. 198.

138 Sentencia del Tribunal Constitucional de España 58/2018, de 4 de junio de 2018 (ECLI:ES:TC:2018:58).

El derecho al olvido no es una categoría jurídica o derecho nuevo o distinto de los ya contemplados y, salvo que en el futuro o el legislador decida reconocerlo con dicha denominación o especificarlo para el caso concreto de las publicaciones en internet, el nombre al uso es el derecho de cancelación de datos personales, recogido en el art. 2 letra h de nuestra Ley Nº 19.628.

El derecho al olvido no es una categoría jurídica o derecho nuevo o distinto de los ya contemplados y, salvo que en el futuro o el legislador decida reconocerlo con dicha denominación o especificarlo para el caso concreto de las publicaciones en internet, el nombre al uso es el **derecho de cancelación de datos personales**, recogido en el art. 2 letra h de nuestra Ley Nº 19.628 como "la destrucción de datos almacenados en registros o bancos de datos, cualquiera fuere el procedimiento empleado para ello", derecho que opera, según el artículo 12 inciso tercero de la misma ley, "en caso de que su almacenamiento carezca de fundamento legal o cuando estuvieren caducos", entre otros. Se trata, desde luego, de uno de los derechosARCO a los que nos refiriéramos anteriormente.

Por eso son incomprensibles sentencias de nuestro país que reclaman, por ejemplo, "que no existe una consagración legal expresa del llamado 'derecho al olvido'"[139], que "no existe ninguna ley que establezca el denominado 'derecho al olvido'" [140], o que "como es sabido, el denominado derecho al olvido que invoca el recurrente no está establecido en nuestra legislación"[141], buscando los jueces en los textos legales conceptos que razonablemente no están ni deberían encontrar y fundando en esa ausencia una decisión judicial.

Guardando las proporciones, es como si una sentencia declarara que el principio *non bis in idem* no está reconocido expresamente en nuestra legislación y no es aplicable, pues no aparece con ese nombre en ninguna ley, cuando en realidad es un principio general del derecho, transversal al sistema jurídico y recogido en múltiples disposiciones legales, que plantea que las personas no pueden ser enjuiciadas o sancionadas dos veces como consecuencia del mismo hecho.

139 Sentencia de la Corte de Apelaciones de Santiago, de 27 de marzo de 2017, dictada en causa rol Nº 127.496–2016; considerando 23.

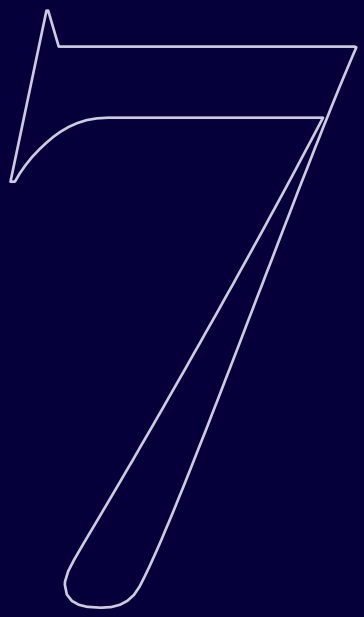
140 Sentencia de la Corte de Apelaciones de Santiago, de 31 de julio 2017, dictada en causa rol Nº 40.773–2017; considerando 9º.

141 Sentencia de la Corte Suprema de Justicia de Chile, de 9 de agosto de 2017, dictada en causa rol Nº 11.746–2017; considerando 4º.

El "derecho al olvido" no es un derecho o una categoría de naturaleza jurídica, sino el nombre periodístico de un atributo fundamental del derecho a la protección de datos contemplado en nuestra Constitución, que en la Ley Nº 19.628 recibe el nombre de "derecho de cancelación".

O bien, acercándolo más todavía al objeto de estudio, que una sentencia chilena declarara que no existe en la ley el derecho a la autodeterminación informativa (denominación doctrinal), porque no ha visto esas palabras en ninguna ley, sin jamás enterarse de que dicho derecho se recoge por las legislaciones positivas como derecho de protección de datos personales.

Reiteramos: el "derecho al olvido" no es un derecho o una categoría de naturaleza jurídica, sino el nombre periodístico de un atributo fundamental del derecho a la protección de datos contemplado en nuestra Constitución, que en la Ley Nº 19.628 recibe el nombre de "derecho de cancelación" y que prescribe, en el artículo 12 inciso tercero de dicha ley, que el titular del mismo "podrá, además, exigir que se eliminen, en caso de que su almacenamiento carezca de fundamento legal o cuando estuvieren caducos".



Eventuales modificaciones a la normativa vigente y su impacto en el control judicial. La situación actual y los cambios que se debaten.

← Índice de contenidos

7.1 Autoridades de control

Los estándares en materia de protección de datos no se limitan a los principios y derechos que deben ser considerados en la legislación, sino que supone la presencia de algo fundamental como es la existencia de una autoridad de protección de datos personales, la cual debe ser independiente y autónoma del poder político, además de contar con una alta calificación técnica.

Tales autoridades de control, por regla general y sin excepciones dignas de mención, son de carácter administrativo y se hacen cargo, por una parte, de promover, educar e informar a los ciudadanos sobre la efectiva vigencia del derecho a la protección de los datos personales, y por otra, de fiscalizar el cumplimiento de la ley y aplicar las sanciones de acuerdo a la naturaleza y gravedad de la transgresión.

Este tipo de autoridades, como el *Garante per la Protezione dei Dati Personali* de Italia, la *Commission Nationale de l'Informatique et des Libertés* de Francia, o la ya mencionada Agencia Española de Protección de Datos, son entes técnicos calificados que deciden en materia derechos, a los cuales las personas pueden recurrir directamente y sin necesidad del patrocinio de un abogado cuando estiman vulnerados sus derechos fundamentales.

En la generalidad de las legislaciones las decisiones que tomen las señaladas autoridades no son finales, sino que son recurribles ante los tribunales ordinarios por quienes consideren que sus derechos han sido injustamente afectados.

Desde luego, no pueden depender del poder político ni estar bajo su subordinación, particularmente cuando es el Estado y los distintos poderes que lo componen, quienes precisamente son uno de los principales tenedores de datos personales al interior del país.

Por supuesto, en la generalidad de las legislaciones las decisiones que tomen las señaladas autoridades no son finales, sino que son recurribles ante los tribunales ordinarios por quienes consideren que sus derechos han sido injustamente afectados.

Ahora bien, la Ley Nº 19.628 de 1999 nunca consideró la existencia de tal autoridad, sino que derivó el conocimiento de las controversias de interés jurídico que pudieran suscitarse a los tribunales ordinarios

de justicia, más precisamente al juez de letras en lo civil del domicilio del responsable del tratamiento, estableciendo un procedimiento especial para ello regulado en el artículo 16 de dicha ley. Lo anterior, generando como efecto secundario que a pesar de que diariamente las personas son objeto de múltiples vulneraciones a sus derechos fundamentales, como situación derivada del tratamiento abusivo de datos personales, en la práctica la cantidad de procedimientos judiciales iniciados por esta causa no sean relevantes o, dicho de otra forma, que las personas queden en desprotección.

Para solucionar lo anterior, el Congreso Nacional refundió los boletines Nº 11.144-07 y Nº 11.092-07 a fin de contar con un proyecto de ley que compatibilizara las visiones del Ejecutivo y del Legislativo, estableciéndose, primero, la creación de una autoridad de protección especializada (así se aprobó en general en el Congreso) para luego, por indicación del Ejecutivo, entregarle tal atribución al Consejo para la Transparencia, que desplegó un intenso *lobby* ante el Ejecutivo para recibir ese rol.

Es así como actualmente, el señalado proyecto de ley dice que "el Consejo para la Transparencia y la Protección de Datos Personales, creado en la ley N° 20.285 sobre Acceso a la Información Pública, será el órgano encargado de velar por el cumplimiento de la normativa relativa al tratamiento de datos personales y su protección, como de todos los derechos consagrados en esta ley".

Sin embargo, como toda ley que no ha concluido su tramitación, no es asunto zanjado, particularmente en circunstancias de que el Consejo para la Transparencia y la Protección de Datos Personales, que decidirá sobre asuntos de derechos, en su designación, de acuerdo al texto actual de la Ley Nº 20.285, es un órgano de composición política que responde a lógicas de cuoteo político-partidista.

Aún más, dentro de las atribuciones previstas para el señalado Consejo están las de aplicar e interpretar administrativamente las disposiciones legales y reglamentarias; fiscalizar y velar por el cumplimiento de los principios, derechos y obligaciones establecidos en la ley; resolver las solicitudes y reclamaciones que formulen los titulares en contra de

los responsables de datos, e investigar y determinar las infracciones en que incurran los responsables de datos y ejercer, en conformidad a la ley, la potestad sancionatoria, entre otras atribuciones.

7.2 El nuevo derecho a la portabilidad de los datos

Como ya se ha mencionado anteriormente, a partir de la entrada en vigencia en 2018 del Reglamento General de Protección de Datos (RGPD) de Europa, que contempla la portabilidad de los datos personales, que "dicho derecho debe aplicarse cuando el interesado haya facilitado los datos personales dando su consentimiento o cuando el tratamiento sea necesario para la ejecución de un contrato. No debe aplicarse cuando el tratamiento tiene una base jurídica distinta del consentimiento o el contrato" (Considerando 68).

Por influencia del señalado Reglamento, este derecho se ha incluido en el proyecto de ley de reforma a la Ley Nº 19.628, a enero de 2021, en estos términos:

> "El titular de datos tiene derecho a solicitar y recibir una copia de los datos personales que le conciernen, que haya facilitado al responsable, en un formato estructurado, genérico y de uso común, que permita ser operado por distintos sistemas y, a comunicarlos o transferirlos a otro responsable de datos, cuando concurran las siguientes circunstancias:
>
> a) El tratamiento se realice en forma automatizada, y
>
> b) El tratamiento esté basado en el consentimiento del titular".

Extrañamente, este es el único supuesto en que se prevé que el responsable de los datos pueda exigir el pago de los costos directos en que incurra por el hecho de acceder a esta solicitud del titular del derecho, lo que arroja sombras sobre el asunto, pues en definitiva se trataría de un derecho constitucional que, en una de sus expresiones concretas, el ciudadano solo puede ejercer si tiene dinero para ello.

7.3 Notificación de vulneraciones de seguridad

Desde hace bastante tiempo se venía discutiendo, en ámbitos académicos, la necesidad de establecer un sistema de notificaciones (*data breach notification*) en caso de que el responsable del tratamiento tuviera problemas como la pérdida o hurto de los datos de las personas, a fin de advertir a estas de tal acontecimiento, de forma que puedan tomar las providencias necesarias para disminuir el impacto o dimensiones del daño.

En ese sentido, el responsable del tratamiento debe comunicar al interesado, sin dilaciones, la violación de la seguridad de los datos personales, particularmente cuando ello puede entrañar un alto riesgo para sus derechos y libertades.

Tal idea, finalmente, se plasmó en el RGPD, en el cual se dispone que su comunicación debe especificar la naturaleza de la violación de la seguridad de los datos personales y las recomendaciones para que la persona afectada mitigue los potenciales efectos adversos.

Es claro que dichas comunicaciones deben realizarse tan pronto como sea posible y en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones o las de otras autoridades competentes, sin perjuicio de aplicar, en paralelo, medidas adecuadas para impedir violaciones de la seguridad de los datos personales continuas o similares.

En Chile, la idea fue incorporada al proyecto de ley que reforma la Ley Nº 19.628, y se ha consignado (hasta el momento) como un "deber de reportar las vulneraciones a las medidas de seguridad", por el cual el responsable y el encargado del tratamiento de los datos deben reportar a la autoridad de protección de datos las vulneraciones a las medidas de seguridad que ocasionen la destrucción, filtración, pérdida o alteración accidental o ilícita de los datos personales, cuando exista un riesgo razonable para los derechos y libertades de los titulares.

Además, se ha establecido que en caso de que dichas vulneraciones se refieran a datos personales sensibles, datos relativos a niños y niñas menores de catorce años o datos relativos a obligaciones de carácter económico, financiero, bancario o comercial, el responsable y el encargado de datos deberán también efectuar esta comunicación a los titulares de estos datos, lo que deberá hacerse en un lenguaje claro y sencillo, singularizando los datos afectados y señalando las posibles consecuencias de las vulneraciones de seguridad y las medidas de solución o resguardo adoptadas.

Como es dable suponer, los responsables de tratamiento que tengan que enfrentar esta contingencia, en principio, no tienen ningún incentivo para dar a conocer los fallos de seguridad, de los cuales posiblemente serán responsables, pero el propio proyecto califica como infracción gravísima omitir en forma deliberada la comunicación de las vulneraciones a las medidas de seguridad que puedan afectar la confidencialidad, disponibilidad o integridad de los datos personales, imponiendo como sanción multas que pueden ir desde las 5.001 a las 10.000 Unidades Tributarias Mensuales, es decir, dentro de un rango que puede llegar a superar los 500 millones de pesos chilenos.

7.4 Régimen infraccional

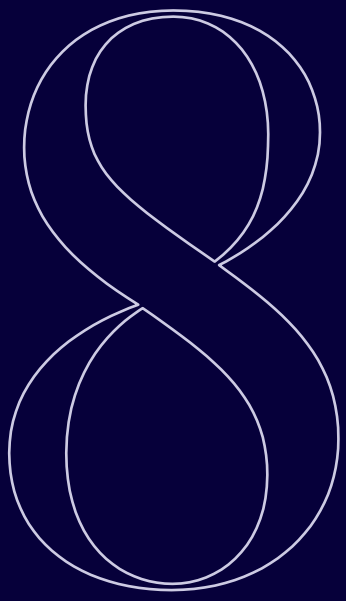
Uno de los talones de Aquiles más conocidos de nuestra actual legislación es la inexistencia de un régimen sancionatorio para los infractores de la Ley Nº 19.628, lo que puede llevar a la convicción de que vulnerar la normativa de protección de datos, salvo respecto de cuestiones de capital reputacional, no conlleva costos mayores asociados, salvo en el remoto caso de que la víctima pueda demostrar ante tribunales un efectivo perjuicio y solicite que se le indemnice.

Lo anterior es una posibilidad muy remota, pues de acuerdo a lo previsto en el procedimiento es la víctima la que debe acompañar todos los medios de prueba necesarios, los que usualmente están asociados a plataformas tecnológicas que desconoce y que no están bajo su control.

El proyecto de ley viene en solucionar esta situación, estableciendo un régimen que diferencia entre **infracciones leves**, como sería omitir la individualización del domicilio postal, del correo electrónico o del medio electrónico equivalente que permita comunicarse con el responsable de los datos o su representante legal; pasando por las **infracciones graves**, como es el tratar los datos personales sin contar con el consentimiento del titular de datos o sin un antecedente o fundamento legal que otorgue licitud al tratamiento, o tratarlos con una finalidad distinta de aquella para la cual fueron recolectados; y concluyendo con las **infracciones gravísimas**, cuyas multas son las más elevadas, como sucedería cuando se efectúa tratamiento de datos personales en forma fraudulenta o cuando se comunica, a sabiendas, información no veraz, incompleta, inexacta o desactualizada sobre el titular de datos.

El proyecto de ley prevé, en estos casos, que las sanciones a las infracciones en que incurran los responsables de datos serán de amonestación escrita o multa de 1 a 100 UTM para las infracciones leves; de 101 a 5.000 UTM para las infracciones graves, y de 5.001 a 10.000 UTM para las infracciones gravísimas.

Pero eso no es todo, porque en casos de reincidencia la autoridad de protección de datos podrá aplicar una multa de hasta tres veces el monto asignado a la infracción cometida; incluso, tratándose de infracciones gravísimas, la señalada autoridad puede disponer la suspensión de las operaciones y actividades de tratamiento de datos que realiza el responsable hasta por un término de 30 días, medida prorrogable indefinidamente si nada se corrige, lo que en los hechos paralizará la empresa o la conducirá a su completa insolvencia.



El tratamiento de datos por el Estado

← Índice de contenidos

8.1 Legitimación para el tratamiento de datos

La Ley Nº 19.628 dispone que los organismos públicos podrán realizar operaciones de tratamiento de datos dentro de la órbita de su competencia y de acuerdo a las condiciones que establece la ley. Siendo así, para el Estado rigen las normas y principios que hemos señalado, con la única particularidad de poder realizar estas operaciones sin necesidad del previo consentimiento del afectado o titular de los datos personales.

Se ha dicho que, por tanto, la Ley Nº 19.628 es la ley que establece la primera legitimación para el tratamiento de datos por parte de organismos públicos, tales como el Ministerio de Educación, el Servicio Nacional de Capacitación y Empleo (Sence), la Junta Nacional de Auxilio Escolar y Becas (Junaeb), las corporaciones de educación municipal, el Ministerio de Salud, Gendarmería de Chile, entre otros, respecto de datos personales generados en o con ocasión del desarrollo de las labores que determinen sus respectivas leyes orgánicas, en la medida que su tratamiento sea necesario para el ejercicio de las funciones que esa ley les prevé.

Es importante destacar que si bien la norma exime al Estado del deber de obtener el consentimiento previo del afectado, en ningún momento autoriza a no informarle sobre el tratamiento de datos que se está realizando. De igual modo, le impone a sus organismos el deber de respeto a los principios de calidad, finalidad, seguridad, responsabilidad, temporalidad, etcétera.

Es importante destacar que si bien la norma exime al Estado del deber de obtener el consentimiento previo del afectado, en ningún momento autoriza a no informarle sobre el tratamiento de datos que se está realizando. De igual modo, le impone a sus organismos el deber de respeto a los principios de calidad, finalidad, seguridad, responsabilidad, temporalidad, etcétera, ya revisados.

Cuando estas entidades no respeten los derechos de acceso, modificación, cancelación o bloqueo en los términos que establece la ley, estarán sujetas al régimen infraccional establecido en ella, conforme al cual, de acogerse por el tribunal una reclamación interpuesta de acuerdo al procedimiento de *habeas data* y luego el organismo público no da cumplimiento a lo dispuesto en la misma, "el tribunal podrá sancionar al jefe del Servicio con la suspensión de su cargo, por un lapso de cinco a quince días" (art. 16 inciso final).

De igual manera, conforme al artículo 23, el organismo público responsable del banco de datos personales deberá indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de los datos, sin perjuicio de proceder a eliminar, modificar o bloquearlos de acuerdo a lo requerido por el titular o, en su caso, lo ordenado por el tribunal.

Estas normas se deben analizar en concordancia con lo dispuesto en el artículo 8º de la Constitución Política de la República, en cuanto establece la transparencia de la información pública. Se hace hincapié en que la obligación constitucional se manifiesta en términos tales que la administración del Estado –durante la puesta a disposición del público– deberá en todo momento respetar los derechos fundamentales de las personas en general y la protección de datos en particular. Siendo así, en aquellos casos que con fines de transparencia sea necesario publicitar información que es objeto de tratamiento con ocasión de las competencias del órgano, debe guardarse especial cuidado en cuanto a los principios antes señalados.

A vía ejemplar, unos años atrás el gobierno publicó la identidad de personas que habían sido beneficiadas con becas de perfeccionamiento o de postgrado. Al respecto, estimamos que si bien es importante que se publiciten tanto los adjudicatarios como los fundamentos de la adjudicación, consideramos relevante para la protección de los derechos de los afectados que la información publicada sea completa y veraz. Por tanto, no bastará con publicitar los antecedentes antes señalados, sino además cuánto tiempo la persona gozó del beneficio, si obtuvo los títulos o grados a los que conducían los estudios financiados a través de dichos recursos, y si los beneficiados cumplieron las obligaciones que estaban consideradas en la beca respectiva, tales como trabajar cierto tiempo en la administración pública, u otras.

Solo así, en una parte, la ciudadanía tomará cabal conocimiento de la información relevante y en otra, se resguardarán los derechos de los afectados.

Otro caso que fue noticia en el año 2020, es el de un médico que se negó a entregar las fichas clínicas de sus pacientes a Fonasa. La Corte Suprema, en autos Nº 21.137-2020, apelación de recurso de

protección, estimó que si bien Fonasa tiene competencias para fiscalizar la modalidad de libre elección, eso no lo habilita para solicitar y revisar las fichas clínicas de los pacientes, pues afecta indebidamente la garantía constitucional consagrada en el artículo 19 Nº 4 de la Constitución Política de la República.

8.2 El tratamiento de datos por los organismos de inteligencia y seguridad

Las fuerzas de orden y seguridad tienen atribuciones para tratar datos personales y en los siguientes acápites nos referiremos a las normas relacionadas a esta materia.

8.2.1 Policía de Investigaciones

El Decreto Ley Nº 2460, ley orgánica de la Policía de Investigaciones de Chile (PDI), establece que será misión de esta policía "investigar los delitos de conformidad a las instrucciones que al efecto dicte el Ministerio Público, sin perjuicio de las actuaciones que en virtud de la ley le corresponde realizar sin mediar instrucciones particulares de los fiscales" (art. 4º).

Luego, el artículo 5º de esta ley dispone lo siguiente:

> "Artículo 5°. Corresponde en especial a Policía de Investigaciones de Chile contribuir al mantenimiento de la tranquilidad pública; prevenir la perpetración de hechos delictuosos y de actos atentatorios contra la estabilidad de los organismos fundamentales del Estado; dar cumplimiento a las órdenes emanadas del Ministerio Público para los efectos de la investigación, así como a las órdenes emanadas de las autoridades judiciales, y de las autoridades administrativas en los actos en que intervengan como tribunales especiales; prestar su cooperación a los tribunales con competencia en lo criminal; prestar la cooperación necesaria en cumplimiento de tratados internacionales ratificados y vigentes en Chile, **incluyendo el intercambio de datos personales**.. Esta cooperación se ajustará a la legislación nacional en la materia y en ningún caso implicará la entrega de bases de datos nacionales ni el acceso directo a ellas por parte de los órganos de un Estado extranjero o de los órganos de una organización internacional, **observando siempre lo dispuesto en la ley Nº 19.628**, sobre Protección de la Vida Privada, particularmente en lo relativo a la protección de los titulares de datos; controlar el ingreso y la salida de personas del territorio nacional; adoptar todas las medidas conducentes para asegurar la correcta identificación de las

personas que salen e ingresan al país, la validez y autenticidad de sus documentos de viaje y la libre voluntad de las personas de ingresar o salir de él; fiscalizar la permanencia de extranjeros en el país, representar a Chile como miembro de la Organización Internacional de Policía Criminal (INTERPOL), y dar cumplimiento a otras funciones que le encomienden las leyes".

En esta materia, el Consejo para la Transparencia se ha pronunciado respecto de las solicitudes de acceso a los datos personales que constan en sus sistemas. Es el caso de la resolución dictada en amparo C-1275-15, en que se solicitó respecto de una persona "si se encuentra en territorio nacional y su último domicilio registrado en Chile. En caso de que no se encuentre en el país, se informe la fecha de salida, paso fronterizo y utilizado y país de destino".

Al respecto, el Consejo resolvió rechazar el amparo, respecto del domicilio, porque "dicho antecedente constituye un dato personal a la luz de la definición prevista en el artículo 2 letra f) de la ley 19.628" y porque "de acuerdo con lo dispuesto por los artículos 4º, 7º y 20 de la citada ley. Su comunicación solo puede efectuarse cuando la ley lo autorice o el titular consienta expresamente en ello. Por lo expuesto, este Consejo concluye que entregar la información pedida afectaría de modo cierto y con la suficiente especificidad los derechos del tercero a quien se refiere la solicitud de información".

Respecto de la segunda solicitud, en cuanto a si la persona se encuentra en Chile y en caso de que no sea así indicar la fecha de salida de Chile, el paso fronterizo y el país de destino, el Consejo estima asimismo que se trata de datos personales. Y agrega que esta información "es obtenida y sometida a tratamiento por la Policía de Investigaciones de Chile, en razón de las contemplado en el decreto ley Nº 2460, del Ministerio de Defensa Nacional, de 1979, no pudiendo comunicar la misma a un tercero que no tenga la calidad de titular del dato que consulta", o que no acredite personería para actuar en su nombre.

8.2.2 Carabineros de Chile

La Ley Nº 8.961, ley orgánica de Carabineros de Chile, en su artículo 2º inciso segundo establece que esta institución tiene "la función

constitucional de garantizar el orden público y la seguridad pública interior". Luego, en el inciso séptimo se refiere al tratamiento de datos personales en los siguientes términos:

> "Corresponderá a la Institución prestar la cooperación necesaria en cumplimiento de tratados internacionales ratificados y vigentes en Chile, **incluyendo el intercambio de datos personales**. Esta cooperación se ajustará a la legislación nacional en la materia y en ningún caso implicará la entrega de bases de datos nacionales ni el acceso directo a ellas por parte de los órganos de un Estado extranjero o de los órganos de una organización internacional, **observando siempre lo dispuesto en la ley N° 19.628**, sobre Protección de la Vida Privada, particularmente en lo relativo a la protección de los titulares de datos".

8.2.3 Agencia Nacional de Inteligencia

La Ley Nº 19.974 "sobre el sistema de inteligencia del Estado y crea la Agencia Nacional de Inteligencia", ley orgánica de la Agencia Nacional de Inteligencia, dispone que el objetivo de este órgano es "producir inteligencia para asesorar al Presidente de la República y a los diversos niveles superiores de conducción del Estado, en conformidad a la presente ley" (art. 7º).

Luego, al enumerar sus funciones y atribuciones, prevé lo siguiente en lo que nos interesa:

> "a) Recolectar y procesar información de todos los ámbitos del nivel nacional e internacional, con el fin de producir inteligencia y de efectuar apreciaciones globales y sectoriales, de acuerdo con los requerimientos efectuados por el Presidente de la República".
>
> (…)
>
> "d) Requerir de los organismos de inteligencia de las Fuerzas Armadas y de las Fuerzas de Orden y Seguridad Pública, así como de la Dirección Nacional de Gendarmería, la información que sea del ámbito de responsabilidad de estas instituciones y que sea de competencia de la Agencia, a través del canal técnico correspondiente. Los mencionados organismos estarán obligados a

suministrar los antecedentes e informes en los mismos términos en que les sean solicitados".

(…)

"e) Requerir de los servicios de la Administración del Estado comprendidos en el artículo 1° de la ley N° 18.575 los antecedentes e informes que estime necesarios para el cumplimiento de sus objetivos, como asimismo, de las empresas o instituciones en que el Estado tenga aportes, participación o representación mayoritarios. Los mencionados organismos estarán obligados a suministrar los antecedentes e informes en los mismos términos en que les sean solicitados, a través de la respectiva jefatura superior u órgano de dirección, según corresponda".

En los mismos términos, esta ley se refiere a las atribuciones de la inteligencia policial en el artículo 22.

En estas circunstancias, muchas veces los organismos públicos son requeridos para celebrar convenios en que requieren datos personales para los efectos de desarrollar sus labores. En todo caso, la Agencia Nacional de Inteligencia deberá custodiar los datos personales que le sean comunicados, adoptando los resguardos necesarios para evitar accesos indebidos, fugas de datos y desviaciones de finalidad.

8.2.4 Protección de datos y actividades de videovigilancia para la mantención de la seguridad pública

Antes de entrar al análisis del tratamiento de datos en este ámbito, es importante considerar que no toda captación de imágenes es considerada videovigilancia[142], pues para que se enmarque dentro de esta categoría el registro debe cumplir con las normas legales y reglamentarias que lo avalen como tal.

142 Al respecto, la ley orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantías de los derechos digitales, en su artículo 22 dispone lo siguiente:
"Tratamientos con fines de videovigilancia.

Existe un consenso bastante amplio en la utilidad de los sistemas de videovigilancia para el resguardo de la seguridad pública, especialmente cuando se teme que puedan producirse atentados de carácter terrorista, tal y como expresa Goñi (2007; p. 16), quien ha sostenido que "las tecnologías de la vigilancia son imprescindibles para luchar contra la amenaza de los grandes atentados, y ese argumento está sirviendo también en los ámbitos particulares y domésticos para hacer frente a los pequeños ataques a la propiedad, como si el concepto de seguridad pasase ineludiblemente por el de videovigilancia. El Estado y el ciudadano recurren a la videovigilancia porque es fuente de información y porque procura una mayor seguridad. En efecto,

1. Las personas físicas o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas o bienes, así como de sus instalaciones.
2. Solo podrán captarse imágenes de la vía pública en la medida que resulte imprescindible para la finalidad mencionada en el apartado anterior.
No obstante, será posible la captación de la vía pública en una extensión superior cuando fuese necesario para garantizar la seguridad de bienes o instalaciones estratégicos o de infraestructuras vinculadas al transporte, sin que en ningún caso pueda suponer la captación de imágenes del interior de un domicilio privado.
3. Los datos serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones. En tal caso, las imágenes deberán ser puestas a disposición de la autoridad competente en un plazo máximo de setenta y dos horas desde que se tuviera conocimiento de la existencia de la grabación.
No será de aplicación a estos tratamientos la obligación de bloqueo prevista en el art. 32 de esta ley orgánica.
4. El deber de información previsto en el artículo 12 del Reglamento (UE) 2017/679 se entenderá cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679. También podrá incluirse en el dispositivo informativo un código de conexión o dirección de internen de esta información.
En todo caso, el responsable del tratamiento deberá mantener a disposición de los afectados la información a la que se refiere el citado reglamento.
5. Al amparo del artículo 2,2 c) del Reglamento (UE) 2016/679, se considera excluido de un ámbito de aplicación el tratamiento por una persona física de imágenes que solamente capten el interior de su propio domicilio.
Esta exclusión no abarca el tratamiento realizado por una entidad de seguridad privada que hubiera sido contratada para la vigilancia de un domicilio y tuviese acceso a las imágenes.
6. El tratamiento de los datos personales procedentes de las imágenes y sonidos obtenidos mediante la utilización de cámaras y videocámaras por las fuerzas y cuerpos de seguridad y por los órganos competentes para la vigilancia y control en los centros penitenciarios y para el control, regulación, vigilancia y disciplina del tráfico, se regirá por la legislación de transposición de la directiva (UE) 2016/680, cuando el tratamiento tenga fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública.
Fuera de estos supuestos, dicho tratamiento se regirá por su legislación específica y supletoriamente por el Reglamento (UE) 2016/679 y la presente ley orgánica.
7. Lo regulado en el presente artículo se entiende sin perjuicio de lo previsto en la ley 5/2014, de 4 de abril, de Seguridad Privada y sus disposiciones de desarrollo.
8. El tratamiento por el empleador de datos obtenidos a través de sistemas de cámaras o videocámaras se somete a lo dispuesto en el artículo 89 de esta ley orgánica".

No toda filmación podrá ser considerada videovigilancia. Para satisfacer los imperativos del debido proceso legal, se requiere la existencia estándares de admisibilidad de los medios probatorios que otorguen certeza jurídico-procesal a las partes, especialmente, los criterios de relevancia, idoneidad y proporcionalidad.

no se puede negar que la vigilancia por videocámara puede estar justificada en la protección de las personas y de la propiedad, y que ha sido decisiva para el desarrollo de investigaciones criminales".[143]

Como señalamos antes, no toda filmación podrá ser considerada videovigilancia. Para satisfacer los imperativos del debido proceso legal, se requiere la existencia estándares de admisibilidad de los medios probatorios que otorguen certeza jurídico-procesal a las partes, especialmente, los criterios de relevancia, idoneidad y proporcionalidad.

Siguiendo a Taruffo (2008; p. 38) podría definirse el criterio de relevancia como "un estándar lógico de acuerdo con el cual los únicos medios de prueba que deben ser admitidos y tomados en consideración por el juzgador son aquellos que mantienen una conexión lógica con los hechos en litigio, de modo que pueda sustentarse en ellos una conclusión acerca de la verdad de tales hechos".

Como podemos apreciar esta valoración no es general y abstracta sino que en cada caso concreto habrá de establecer y analizar si entre un determinado elemento de juicio (fuente de prueba) y la aseveración cuya verdad debe determinarse existe una "relación de relevancia", dada por la relación de inferencia entre el hecho comunicado por la fuente de prueba y el hecho afirmado por la parte del proceso. Luego, la existencia entre el hecho a probar y el hecho probatorio define la relevancia de la prueba de que se trate (Taruffo, 2002; p. 442).

Ahora bien, Cepeda (2008; p. 159), en relación al derecho colombiano, ha definido el principio de proporcionalidad como "una prohibición de exceso o defecto". Al respecto, Clerico (2007; p. 149) se refiere al examen de proporcionalidad en sentido amplio, sosteniendo que "la validez del derecho en oportunidad de su limitación significa que a) los derechos actúan como límites a su limitación, y b) elevan una pretensión de ejercicio. Por ello la validez de los derechos impone

143 GOÑI SEIN, José L.: *La videovigilancia empresarial y la protección de datos personales", 1º ed*. Madrid, Thomson Civitas, 2007; p. 16.

límites frente a un exceso de restricción, como así también frente a una acción o acción insuficiente que imposibilite injustificadamente su ejercicio".

Alexy[144] (2003; pp. 101-103), respecto al principio de proporcionalidad como mandato de optimización, señala "que la teoría de los principios implique el principio de proporcionalidad significa que sus tres subprincipios, es decir los subprincipios de idoneidad, necesidad y proporcionalidad en sentido estricto, se siguen lógicamente de ella, o sea son deducibles de ella en un sentido estricto. Por lo tanto, quien objeta la teoría de los principios tiene también que objetar el principio de proporcionalidad"…"los principios exigen la máxima realización posible, en relación con las posibilidades fácticas y jurídicas. La relación con las posibilidades fácticas conduce a los subprincipios de idoneidad y necesidad… en cambio, el principio de proporcionalidad en sentido estricto se origina a partir del mandato de máxima realización posible en relación con las posibilidades jurídicas, sobre todo en relación con los principios que juegan en sentido contrario".

Bernal[145] (2005; pp. 67-68), en base a la jurisprudencia alemana, sostuvo que "toda intervención en los derechos fundamentales que no observe las exigencias de estos subprincipios (del principio de proporcionalidad) es ilegítima y, por tanto debe ser declarada inconstitucional. La aplicación del principio de proporcionalidad presupone que una medida del poder público represente una intervención en un derecho fundamental, es decir, lo afecte negativamente, bien sea anulando, aboliendo, restringiendo o suprimiendo una norma o una posición que pueda ser adscrita prima facie a la disposición constitucional que tipifica el derecho intervenido. Si la medida de intervención supera el test de los subprincipios de proporcionalidad, tal medida será válida definitivamente como una restricción al derecho correspondiente. En caso contrario, la norma o la posición del derecho fundamental objeto de la intervención adquiere una

144 ALEXY, Robert: *Tres escritos sobre derechos fundamentales y la teoría de los principios*, Ed. Universidad Externado de Colombia. Bogotá, 2003.

145 BERNAL, Carlos: "Racionalidad, proporcionalidad y razonabilidad en el control de constitucionalidad de las leyes". En Bernal, C., *El derecho de los derechos*, Ed. Universidad Externado de Colombia. Bogotá, 2005.

validez ya no solo prima facie, sino también definitiva, y por ello una ley que incide negativamente en el derecho debe ser declarada inconstitucional".

Prieto[146] (2007; pp. 99-146) al analizar el principio de proporcionalidad, lo divide en cuatro elementos o subprincipios:

i. **Finalidad:** frente a una medida limitadora del derecho a la prueba, habrá de verificarse si esa medida persigue un fin constitucionalmente legítimo. Si no cumple este requisito sería una limitación **inconstitucional**.

ii. **Adecuación:** la medida constitucionalmente admisible debe ser "conducente", "acertada", apta para la consecución de dicho fin. Si la medida de que se trate no cumple el requisito de adecuación en relación al fin, la limitación no encuentra sustento en el derecho a la prueba y por tanto se torna **ilegítima**.

iii. **Necesidad:** La medida limitadora que cumple las dos condiciones anteriores debe ser la única que, obteniendo los mismos resultados, resulte **menos lesiva** respecto del derecho limitado

iv. **Proporcionalidad en sentido estricto:** implica la exigencia de acreditar una relación de **equilibrio** entre los beneficios a obtener con la medida limitadora y la lesión propiciada al derecho afectado por la limitación.

De nuestra parte, consideramos que además de estas condiciones se deben cumplir con aquellas que se derivan de la aplicación de las normas de tratamiento de datos personales, a saber:

- Que se cumplan los principios de **limitación de la finalidad y minimización de datos** del artículo 5.1 RGPD, apartados b) y c)
- Que se cumplan los principios de **lealtad, licitud y transparencia**.

146 PRIETO, Luis: "El juicio de ponderación constitucional". En M. Carbonell, *El principio de proporcionalidad en el Estado constitucional*. Bogotá, Universidad Externado de Colombia, 2007.

- Que los datos sean recogidos y tratados con **fines determinados, explícitos y legítimos**.
- Que los datos que se recojan sean **adecuados, pertinentes y no excesivos** en relación a la finalidad legítima informada.
- **Registro de actividades** de tratamiento (art. 30 RGPD).
- Adopción de las **medidas de seguridad** (art. 32 RGPD).
- Si se trata de un dron o un globo de vigilancia que opera en recintos privados, se deberá además cumplir con el principio de **información a los titulares** de datos personales (art. 13 RGPD).

Adicionalmente, deberán cumplirse las condiciones específicas, previstas en relación a la operación de drones. En el caso chileno, las normas de la Dirección General de Aeronáutica Civil.

Sobre el asunto, el Consejo para la Transparencia, en amparo 2493-15, se pronunció ante una solicitud de acceso a la información pública respecto de "las grabaciones captadas por los globos aerostáticos ubicados en la comuna de Las Condes, correspondientes al día 20 de agosto entre las 16:00 y 17:00". El Consejo, por unanimidad, rechazó el amparo deducido "por concurrir la causal de secreto o reserva establecido en el artículo 21 Nº 2 de la ley de transparencia [*Nº 20.285*], a excepción del voto concurrente del Consejero don Marcelo Drago Aguirre, quien estima que los antecedentes consultados deben mantenerse bajo reserva, atendido lo dificultoso de efectuar divisibilidad entre las imágenes captadas en espacios públicos respecto de aquellas obtenidas en espacios privados".

El Consejo precisa luego que "la entrega de imágenes captadas por cámaras de vigilancia implica por parte del órgano reclamado un tratamiento de datos personales y, también, de datos de carácter sensible, actividad que puede redundar en afectaciones concretas al derecho a la privacidad y al derecho a la propia imagen, de lo cual deriva la necesidad de garantizar la protección de dichos datos conforme a nuestro ordenamiento jurídico, velando por el adecuado cumplimiento de la ley 19.628".

8.3 Autorización para realizar tratamiento de datos personales por otros organismos públicos

8.3.1 Defensoría de la Niñez

Este organismo ha sido dotado de competencias para tratar datos personales en la Ley Nº 21.067, en concordancia con el artículo 20 de la Ley Nº 19.628. La Defensoría de la Niñez tiene como objeto "la difusión, promoción y protección de los derechos de que son titulares los niños, de acuerdo a la Constitución Política de la República, a la Convención sobre los Derechos del Niño y a los demás tratados internacionales ratificados por Chile que se encuentren vigentes, así como a la legislación nacional, velando por su interés superior" (art. 2º).

En ese contexto, el artículo 4º letra e le otorga las siguientes funciones y atribuciones, en lo que nos interesa:

> "Requerir antecedentes o informes a los órganos de la Administración del Estado o a aquellas personas jurídicas que tengan por objeto la promoción o protección de los derechos de los niños, cuando, dentro del ámbito de sus competencias, tome conocimiento, de oficio o a petición de parte, de posibles vulneraciones a tales derechos por actos u omisiones de las entidades. Para tales efectos, el requerimiento deberá establecer un plazo razonable para la entrega de la información solicitada, el que no superará los sesenta días corridos".

Como es posible apreciar, este artículo no alude expresamente a la facultad de tratar datos personales, sin embargo sí se refiere a requerir antecedentes o informes, relacionados con niños, niñas y adolescentes específicos. Asimismo, la posibilidad de que este organismo trate datos personales se desprende de lo dispuesto en el artículo 8º de esta misma ley, relativo a las obligaciones de la Defensoría, especialmente la de respetar el principio de finalidad y el pleno respeto a los derechos de los titulares de los datos personales, como podemos ver a continuación:

> "Artículo 8°. La información y antecedentes recibidos por la Defensoría no podrán ser empleados para fines ajenos al ámbito

de sus competencias. Su tratamiento deberá siempre respetar los derechos y las garantías constitucionales y legales, especialmente lo dispuesto en la Ley N° 19.628, sobre Protección de la Vida Privada".

8.3.2 Instituto Nacional de Derechos Humanos

Conforme a la Ley N° 20.405, que crea el Instituto Nacional de Derechos Humanos, el Instituto tiene por objeto la promoción y protección de "los derechos humanos de las personas que habiten en el territorio de Chile, establecidos en las normas constitucionales y legales; en los tratados internacionales suscritos y ratificados por Chile y que se encuentran vigentes, así como los emanados de los principios generales del derecho, reconocidos por la comunidad internacional. En su organización interna se regirá por las disposiciones de esta ley y lo que señalen sus estatutos" (art. 2º).

Para el cumplimiento de sus finalidades, el INDH podrá celebrar convenios de colaboración y cooperación con organismos públicos y privados, nacionales o internacionales, dentro del ámbito de sus competencias.

El INDH tiene atribuciones para tratar datos, aun cuando en su ley se refiere a "información", conforme establece el artículo 3º Nº 6, en los siguientes términos:

"En el cumplimiento de este objetivo, deberá recopilar, analizar y sistematizar toda información útil a este propósito; también podrá solicitar información acerca del funcionamiento de los mecanismos reparatorios e impulsar, coordinar y difundir acciones de orden cultural y simbólico destinados a complementar el respeto a los derechos humanos y a reivindicar a las víctimas y a preservar su memoria histórica.

Asimismo, solicitar, reunir y procesar el conjunto de la información existente en poder de entes públicos o privados, que diga relación con las violaciones a los derechos humanos o la violencia política a que se refiere el Informe de la Comisión Nacional de Verdad y Reconciliación, sin perjuicio de lo dispuesto en el inciso primero".

8.3.3 Servicio Electoral

De acuerdo al artículo 1º de la ley orgánica del Servel, este servicio tiene acceso directo a los datos electorales de todas las personas registradas en el Servicio de Registro Civil e Identificación:

> "Se entenderá por datos electorales de chilenos y extranjeros residentes: los nombres y apellidos, el número de rol único nacional, la fecha de nacimiento, el lugar de nacimiento, la nacionalidad, el sexo, la profesión y el domicilio. También son datos electorales los antecedentes necesarios para determinar si una persona ha perdido la ciudadanía y el derecho a sufragio, o si este se encuentra suspendido.
>
> El Servicio Electoral usará estos datos con el solo objeto de realizar estudios y pruebas sobre incorporaciones electorales automáticas; deberá mantener en absoluta reserva y confidencialidad la información y documentación que obtenga en virtud de esta disposición y garantizar, en todo momento, la protección de los datos de carácter personal regulados en la ley N° 19.628, sobre protección de la vida privada".

Si bien hay otros organismos públicos cuyas leyes orgánicas han establecido normas específicas de tratamiento de datos personales, hemos tratado de reseñar una muestra representativa, que permita comprender la mecánica en la aplicación coherente entre las normas específicas o sectoriales y la ley de protección de datos personales.

8.4 Tratamiento de datos personales y la prueba en juicio

En el ámbito procesal, se realizan tratamientos de datos personales ya sea por el tratamiento de datos que realiza el Poder Judicial en el manejo de expedientes o, en lo que nos interesa, en ámbitos extra-procesales, con ocasión de la preconstitución de pruebas, lo cual ha cobrado relevancia en el contexto de la implementación de sistemas de videovigilancia en la ciudad.

8.4.1 Tratamiento de datos de imágenes y video para preconstitución de pruebas en juicios civiles

En materia civil, la videovigilancia se ha empleado tanto en la preconstitución de pruebas como en la producción de las mismas durante el proceso, y estas son operaciones de tratamiento de datos personales.

En este caso, para identificar los criterios de legitimidad-licitud analizaremos la sentencia 10764/09 dictada por el TEDH, de 27 de mayo de 2014.[147] El solicitante era un español que, luego de verse involucrado en un accidente de tráfico, adujo a la compañía de seguros que como resultado del mismo ahora estaba impedido de conducir vehículos motorizados. La compañía contrató detectives privados, quienes realizaron grabaciones del solicitante manejando una motocicleta, las cuales fueron presentadas y aceptadas como prueba por el tribunal. El solicitante estimaba que esta prueba era ilícita, porque no se le solicitó su consentimiento para realizar las grabaciones.

El TEDH sostuvo que la grabación de imágenes de video constituye una injerencia en la vida privada y que la imagen personal es uno de los atributos principales de la personalidad, que revela su originalidad y le permite a una persona diferenciarse de sus congéneres, por lo que se reconoce la posibilidad para el individuo de rechazar

147 TEDH, demanda Nº 10764/09, De La Flor Cabrera c. España.

la captura, conservación y difusión de su imagen[148]; luego, se refirió a la necesidad de que se establezca un **justo equilibrio** entre los derechos e intereses en juego.

Respecto de la captura de imágenes, el TEDH considera que las filmaciones fueron legítimas por las siguientes razones:

- **En cuanto a las capturas:** se realizaron tomas circunstanciales y no se efectuó un seguimiento permanente; las imágenes fueron tomadas en la vía pública, por lo que no incluyen escenas relativas a la vida cotidiana del demandante ni se realizó ninguna interferencia en el comportamiento de la persona.
- **En relación a su difusión:** se utilizaron exclusivamente como medio de prueba en el juicio respectivo, con la finalidad de "contribuir de manera legítima al debate judicial" y "aportar al juez el conjunto de los elementos pertinentes", sin que estuvieran destinadas a ser publicadas, por lo que no había riesgo de una explotación posterior.
- **En relación al agente**: las filmaciones fueron realizadas por una agencia de detectives privados debidamente habilitada para realizar esta actividad de acuerdo al derecho interno de España.

8.4.2 Tratamiento de datos de videovigilancia como prueba en los juicios laborales

En materia laboral, la videovigilancia se fundado en la necesidad de garantizar la seguridad del entorno de trabajo y de paso la de monitorear las actividades de las personas que laboran en él. En su empleo deberán respetarse los derechos fundamentales del trabajador.[149]

Consistentemente, las cámaras solo podrán instalarse en espacios "**laborales**", no en áreas de descanso o esparcimiento de los trabajadores ni en zonas en las cuales desarrollen actividades privadas. Asimismo, no podrán programarse para seguir un **objetivo específico**, sino que

148 TEDH, demanda Nº 10764/09, De La Flor Cabrera c. España. (FJ 30 y 31).
149 Véase por ejemplo las SSTC 98/2000 de 10 de abril, fundamento jurídico 7, y SSTV 308/2000, de 18 de diciembre, FJ 430 de noviembre (fj.18).

deberán grabar planos generales. Adicionalmente, se ha proscrito la **videovigilancia encubierta**. En el caso español, así lo ha previsto la normativa laboral[150] y la de protección de datos personales.[151]

En este mismo sentido, la STC 186/2000, de 10 de julio, sostuvo que estos sistemas debían cumplir los siguientes requisitos para considerarse aceptable:

- **Idoneidad:** la medida debe ser capaz de conseguir el objetivo propuesto.
- **Necesidad:** se requiere el empleo de la medida es necesaria para lograr el objetivo perseguido.
- **Proporcionalidad:** debe existir un equilibrio entre afectar el derecho fundamental y la importancia del fin legítimo buscado, el cual se cumpliría al limitar la medida a los espacios y tiempo estrictamente necesarios en relación a la finalidad y, tratándose de

150 Al respecto véase el Estatuto de los Trabajadores de España, Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores, que en su artículo 20 bis dispone: "Derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión. Los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales".

151 Al respecto, la ley orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantías de los derechos digitales, en su artículo 89 dispone lo siguiente: "Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo.
1. Los empleadores podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los trabajadores y en la legislación de función pública, siempreque estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. Los emplea- dores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o losempleados públicos y, en su caso, a sus representantes, acerca de esta medida.
En el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el 22.4 de esta ley orgánica.
2. En ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos.
3. La utilización de sistemas similares a los referidos en los apartados anteriores para la grabación de sonidos en el lugar de trabajo se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores. La supresión de los sonidos conservados por estos sistemas de grabación se realizará atendiendo a lo dispuesto en el apartado 3 del artículo 22 de esta ley".

> la videovigilancia en el trabajo, que al menos existan razonables sospechas respecto de los hechos que se busca indagar, por parte de quien emplea la medida.

Luego, la STC 39/2016 aplicaría estos mismos criterios tratándose de las videocámaras debidamente informadas a los trabajadores.[152]

Con la entrada en vigor de las leyes de protección de datos en España, la STC 29/2013, de 11 de febrero, agregó a los requisitos anteriores que la instalación permanente de cámaras de videovigilancia por motivos de seguridad requiere la **notificación previa** a los representantes sindicales y empleados, bajo sanción de constituir una violación a lo previsto en el artículo 18.4 de la Constitución española.

A esta misma conclusión ha arribado la autoridad administrativa en Chile, a partir de lo dispuesto en el artículo 5º del Código del Trabajo.[153] A vía ejemplar, el Ord. Nº 2875/72, de 22 de julio de 2003, con ocasión de un empleador que instaló "16 cámaras fijas en el exterior de las instalaciones (patios) y 16 en su interior (solo en el área de producción), contando con algunas cámaras enfocadas directamente a los procesos productivos o áreas específicas y otras 'cámaras domo', con un amplio radio de captación de imagen, además de dos operadores".

152 En lo pertinente, en su fundamento jurídico número 5, la sentencia 39/2016 del Tribunal Constitucional, de 3 de marzo de 2016, consideró que "...el uso de cámaras de seguridad fue justificado (ya que existía una sospecha razonable que algunos de los empleados robaban efectivo de la caja), apropiado (para verificar si estas irregularidades estaban siendo cometidas por algunos de los empleados, y en tal caso, adoptar las medidas disciplinares apropiadas), necesario (la videovigilancia se utilizaría como prueba de dichas irregularidades) y proporcional (la grabación se limitó a la zona donde se encontraba la caja).

153 El artículo 5º DFL 1, de 2002 (versión de 28.11.2018), dispone: "El ejercicio de las facultades que la ley le reconoce al empleador, tiene como límite el respeto a las garantías constitucionales de los trabajadores, en especial cuando pudieran afectar la intimidad, la vida privada o la honra de estos.
Los derechos establecidos por las leyes laborales son irrenunciables, mientras subsista el contrato de trabajo. Los contratos individuales y los instrumentos colectivos de trabajo podrán ser modificados, por mutuo consentimiento, en aquellas materias en que las partes hayan podido convenir libremente".

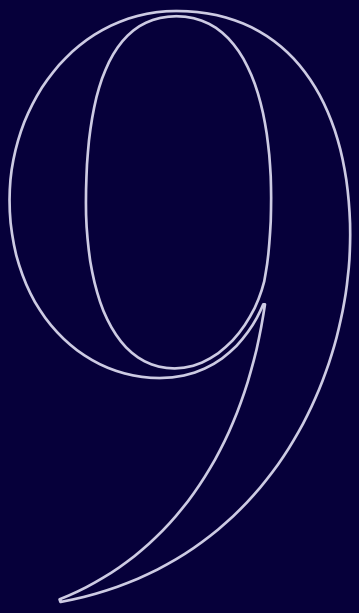
En este caso, la finalidad declarada fue la necesidad de mantener un nivel de seguridad que permitiera evitar atentados desde el exterior de la empresa y al proceso productivo mismo, así como asegurar la producción y su manipulación, objetivos que se habrían logrado, según la empresa.

Pues bien, el organismo fiscalizador consideró que, a la luz del artículo 5º del Código del Trabajo ya citado, "la utilización de mecanismos de control audiovisual (grabaciones por videocámaras)… solo resulta lícita cuando ellos **objetivamente se justifican** por requerimientos o exigencias técnicas de los procesos productivos o por razones de seguridad…, y por tanto el control de la actividad del trabajador solo puede ser 'un resultado secundario o accidental del mismo'", nunca como la intención primaria del empleador.

Respecto de la finalidad, sostuvo que la seguridad como justificación del sistema se limita a la seguridad de las **personas,** de las **instalaciones** o cuando el **proceso productivo** así lo exija desde el punto de vista técnico.

Adicionalmente, **proscribe el control empresarial permanente y continuado,** por provocar en el trabajador "inexorablemente, un estado de tensión o presión incompatible con la dignidad humana" y vulnerar la esencia misma de su libertad y autodeterminación, al impedirle, en los hechos, la más mínima licencia de comportamiento.

Por tanto, la autoridad considera que el **principio de proporcionalidad** "se traduce en un examen de admisibilidad –ponderación– de la restricción que se pretende adoptar basado en la valoración del medio empleado –constricción del derecho fundamental– y el fin deseado –ejercicio del propio derecho–".



Desafíos de la protección de datosen el tránsito a la automatización

← Índice de contenidos

9.1 El fenómeno de la minería de datos y el bigdata y las formas de control judicial

La predicción del comportamiento humano ya no es asunto de mentalistas y está muy lejos de ser brujería. A través de operaciones de *big data*, se realiza el tratamiento de grandes volúmenes de información veraz, variada, en un tiempo mínimo o velozmente, generando así nueva información valiosa para los procesos de toma de decisiones.

Para ello, los sistemas informáticos rastrean, recolectan y procesan información de manera constante, gracias a la cantidad ingente de dispositivos conectados que usa una persona y de los servicios de la sociedad red que utiliza en su vida diaria, algunos incluso sin tener conciencia respecto de ello. Y a esto se suman los complejos sistemas de vigilancia activa y pasiva, que abundan en nuestras ciudades "inteligentes".

Los datos son comunicados a través de las redes y sistemas de comunicaciones electrónicas, almacenados en grandes sistemas de información, generalmente distribuidos y luego procesados en base a complejos algoritmos de análisis y decisión. Todo ello, en fracciones de segundos, casi en tiempo real.

A diferencia de los primeros tiempos de la computación, no es necesario que los datos se estructuren en sistemas de bases de datos previamente diseñados y parametrizados. Basta recoger la información en el estado que se encuentre, luego un motor de búsqueda encontrará patrones, los clasificará y analizará en busca de información valiosa para los agentes que se sirven de estos sistemas.

En este contexto, cobra relevancia el rol de la inteligencia artificial (IA) y sus métodos de funcionamiento, así como el uso de los algoritmos, esto es, el conjunto de normas o reglas específicas que indican los pasos a seguir en el procesamiento de la información para su análisis y obtención de resultados.

Otro aspecto esencial dice relación con la existencia de técnicas y programas que dotan de capacidad de aprendizaje automático a los sistemas (*machine learning*). Al respecto, hoy en día las máquinas, además de desarrollar aprendizaje supervisado, a través de técnicas tales como la clasificación y la regresión, también se las ha dotado de la capacidad de aprender de manera no supervisada.

En este sentido, se habla de aprendizaje profundo (*deep learning*) para agrupar las técnicas que emulan redes neuronales, dotando a los sistemas de altas capacidades de aprendizaje mediante el empleo de técnicas de aprendizaje automático que explotan simultáneamente muchas capas de procesamiento.

Como en todo proceso de aprendizaje, los sistemas se entrenan, usualmente a través del ingreso de datos históricos del proceso que se desea analizar, y se les dota de reglas de cálculo. Luego se realiza el procesamiento y se verifica si los datos de salida corresponden en mayor o menor medida a los resultados reales conocidos del proceso.

Este mismo método se aplica, por ejemplo, en la predicción de consumo de las personas o en la probabilidad de que cumplan sus obligaciones financieras, entre otras finalidades, pero lo que nos interesa aquí son todas aquellas que dicen relación con el tratamiento de datos personales.

Al respecto, uno de los aspectos que más críticas ha levantado es la falta de transparencia de los algoritmos, en el sentido de que no relevan los datos que consideran ni las fórmulas o los factores aplicados para sopesarlos. En efecto, estos procesamientos de información pueden conducir a decisiones erróneas o derechamente arbitrarias, debido a múltiples factores.

En primer lugar, puede ser que las muestras de datos de aprendizaje hayan sido parciales, no representativas o derechamente falsas, o puede que los factores aplicados no tengan el peso específico correcto, por mencionar algunos de los aspectos que podrían llevar a que se acuse de sesgado al algoritmo.

A vía ejemplar, algún tiempo atrás la empresa Amazon creó un sistema automatizado de selección de personal. En la fase de aprendizaje, se ingresaron los datos relativos a los perfiles de las personas que históricamente habían desempeñado los distintos perfiles de cargo en la compañía, y con ello el sistema aprendió que los puestos gerenciales debían ser ocupados por personas de sexo masculino, de origen educacional de elite y de raza blanca, perpetuando así una tendencia arbitrariamente discriminatoria.

En nuestro país, el caso del algoritmo de cálculo de riesgo comercial, de la empresa Dicom, es un ejemplo de la incorporación de datos no pertinentes en el cálculo del riesgo. Consideraba como variable las consultas realizadas por terceros respecto de una persona, puntuando negativamente la circunstancia de que muchas personas consultaran los antecedentes de alguien. En su momento, Dicom sostuvo que la inclusión de este tipo de información agregaba valor predictivo útil, pero sus detractores adujeron que no había evidencia de que esa información fuera objetiva o racional, pues se origina en la acción de terceros distintos del titular de los datos personales, los cuales podrían, de manera mal intencionada, generar consultas para los efectos de hacer caer el puntaje de la persona afectada.

Por nuestra parte, estimamos que el *scoring* o puntaje que utilizan, por ejemplo, las oficinas de información crediticia, es un dato personal, por cuanto se refiere o atribuye a una persona determinada o determinable y, por tanto, queda sujeta a las normas sobre protección de datos personales.

La primera consecuencia de esta calificación es que la persona debe tener la posibilidad de conocer (*acceso*) tanto el predictor, como la información relativa a los datos incluidos en el cálculo y los factores de ponderación aplicados. Tendrá asimismo el derecho de solicitar la rectificación (*modificación*) de los resultados, solicitar su cancelación y bloquear el acceso a esta información, si está siendo objeto de un tratamiento abusivo. Adicionalmente, la persona debe tener la posibilidad de impugnar la decisión si esta ha sido en un ciento por ciento automatizada.

Si bien es evidente la necesidad de proteger los datos sobre evaluaciones y predicciones relativas a una persona, sobre todo porque a partir de ellos pueden tomarse decisiones arbitrarias a su respecto, la legislación chilena vigente se refiere a ellos solo respecto de la evaluación de riesgo comercial.

Esto genera una paradoja, en el sentido de que si bien es evidente la necesidad de proteger los datos sobre evaluaciones y predicciones relativas a una persona, sobre todo porque a partir de ellos pueden tomarse decisiones arbitrarias a su respecto, la legislación chilena vigente se refiere a ellos solo respecto de la evaluación de riesgo comercial.

La paradoja ocurrió a partir de la entrada en vigor de la Ley Nº 20.591, que modificó el artículo 9º de la Ley Nº 19.628 introduciéndole el siguiente inciso final:

> "Prohíbese la realización de todo tipo de **predicciones o evaluaciones de riesgo comercial** que no estén basadas únicamente en información objetiva relativa a las morosidades o protestos de las personas naturales o jurídicas de las cuales se informa. La infracción a esta prohibición obligará a la eliminación inmediata de dicha información por parte del responsable de la base de datos y dará lugar a la indemnización de perjuicios que corresponda".

Uno de los factores gatillantes de esta modificación fue considerar, como se señaló más atrás, que el algoritmo de la principal empresa de elaboración de estos perfiles (Dicom/Equifax) consideraba las consultas al número de identificación de la persona en la fórmula de cálculo, por lo que podría decirse que fue una ley reactiva a una situación concreta.

Pero, probablemente, dicha ley era innecesaria: antes de que el proyecto de ley se discutiera, acertadamente un fallo de la Corte de Apelaciones de Santiago, recaído en autos rol Nº 3937-2010, consideró que el predictor de riesgo de la recurrida (Dicom/ Equifax) "vulnera las garantías constitucionales consagradas en los números 2, 4 y 26 del artículo 19 de la Carta Fundamental", para luego sostener que "no obstante la conciencia de estos sentenciadores en cuanto al efecto relativo de las sentencias, no puede omitir el dejar constancia de su parecer en el sentido de que resultan tan obvias las ilegalidades y arbitrariedades que comete la recurrida, con la elaboración y puesta a disposición del público del denominado 'predictor de riesgo', sosteniendo que se trataba de una práctica a la que debiera ponerse término, para evitar así el poder llegar a dañar injustamente el cré-

dito y la imagen de las personas, pues estimaban que esta actividad carecía de autorización legal para su realización, sin que existieran razones objetivas que lo avalaran".

Como se puede apreciar, la Corte estimaba que la legislación vigente a la época no consideraba la elaboración de perfiles como una actividad lícita, pero al dictar el legislador una ley reactiva, no solo legitimó la elaboración de perfiles y con esto una nueva categoría de datos personales –"los datos personales apreciativos"– sino que además solo impuso condiciones a un cierto tipo de predictores, como son los evaluadores de riesgo comercial, dejando en libertad a los demás en el tiempo del desarrollo de las tecnologías *big data*.

¿Qué es un dato apreciativo? Es aquel que se elabora como una construcción realizada por un tercero distinto del titular de los datos, a partir de la información relativa a la persona, su entorno o las actividades que realiza.

¿Qué es un dato apreciativo? Es aquel que se elabora como una construcción realizada por un tercero distinto del titular de los datos, a partir de la información relativa a la persona, su entorno o las actividades que realiza. La apreciación resultará de la aplicación a los datos obtenidos por uno o más algoritmos, automatizados o no.

Como hemos señalado, en entornos que se toman más en serio los derechos de las personas, se ha tenido especial interés en la objetivación y transparencia de los criterios empleados en la construcción de estos indicadores, los cuales, en todo caso, deben responder a los principios generales que rigen el tratamiento de datos personales.

9.2 El "targeting", los algoritmos y la predicción de consumo

El etiquetado (*targeting*) y clasificación de las personas en base a sus hábitos, creencias y deseos, es una de las labores en que los algoritmos han cobrado gran relevancia.

En este caso, se trata de la aplicación de las técnicas que vimos antes, ahora para predecir los comportamientos de consumo de las personas, o persuadirlos o condicionarlos en el sentido que convenga a quien las emplea.

Estas técnicas, en combinación con los mecanismos de georreferenciación, se aplican también para monitorear a los "activos", esto es, a las entidades que se mueven de un lado a otro. Es por ello que nuestro dispositivo móvil puede avisarnos cuánto tardaremos al lugar que estima que nos dirigimos cuando emprendemos la marcha.

En el ámbito penal, se aplican estas técnicas para controlar la proximidad de dos "activos" respecto de los cuales existe un imperativo de mantenerlos a distancia, por existir una orden de alejamiento; también, para verificar si una persona abandona el lugar en que debe cumplir una medida de reclusión domiciliaria, entre otros objetivos.

Al respecto, debe resguardarse que en la aplicación de estas medidas se tomen las providencias necesarias para que no se constituyan en un trato inhumano o degradante, y para que no se afecte indebidamente la honra y la privacidad del sujeto y de su entorno más próximo.

Nos centraremos en este último ámbito, por considerarlo el más crítico respecto de los derechos fundamentales. El mecanismo de recogida de datos y control de personas más utilizado para esta finalidad es el llamado "brazalete electrónico", que transmite información respecto del portador y su entorno que reviste el carácter de dato personal, pues corresponde a información relativa a personas identificadas (sus portadores) o identificables (su entorno).

La información obtenida a partir de estos dispositivos puede ser calificada como datos sensibles, es decir, aquellos que precisan medidas especiales de protección, pues aparte de poder afectar la esfera más íntima de las personas, la información que se conoce a través de ellos podría dar origen a discriminaciones ilegales o arbitrarias del entorno social.

Respecto de estos datos, se realizan operaciones de tratamiento desde su recogida, almacenamiento, comunicación, cancelación, etcétera, las cuales se desarrollan, en último término, bajo responsabilidad del Estado, ya sea que este efectúe el tratamiento por sí mismo o que haya abierto el mercado para dar cabida a prestadores de servicios. A este respecto, deberán observarse las normas de la Ley Nº 19.628, sobre protección de datos personales, en concordancia con lo previsto en la Ley Nº 18.216, que establece penas sustitutivas a las penas privativas o restrictivas de libertad.

La información obtenida a partir de estos dispositivos puede ser calificada como datos sensibles, es decir, aquellos que precisan medidas especiales de protección, pues aparte de poder afectar la esfera más íntima de las personas, la información que se conoce a través de ellos podría dar origen a discriminaciones ilegales o arbitrarias del entorno social.

Entonces, de acuerdo a los principios generales de protección de datos, existen deberes de lealtad, legalidad y respeto a los derechos y libertades de las personas, no solo respecto del portador del dispositivo telemático, sino que de todo su entorno familiar y social, pues en la práctica se puede procesar y relacionar información atingente a todos ellos: fechas, lugares, comportamientos, alzas de presión sanguínea, esfuerzo, entre otros. Lo anterior tiene consecuencias jurídicas, ya que si bien el grillete lo lleva solo una persona, el entorno –al menos el más cercano– no tiene obligaciones de soportar carga alguna, lo que nos conduce a pensar que se deberá obtener su consentimiento expreso para el tratamiento de la información.

Es importante señalar que debe verificarse que se cumpla estrictamente con los fines para los que se estableció la obligación de cargar con un dispositivo telemático, pues el procesamiento de datos incompatibles con los fines perseguidos también requerirá de consentimiento expreso. Es decir, sin autorización judicial no podrían utilizarse los datos obtenidos a través de estos medios para iniciar investigaciones criminales o de otra especie respecto de personas distintas a las directamente controladas o vigiladas, pues de alguna forma los dispositivos telemáticos son también sistemas de "escucha".

Es relevante también velar por el principio de proporcionalidad, lo que en concreto significa que los datos en cuestión deben ser adecuados, relevantes y no excesivos. Así por ejemplo, si la sanción implica cumplir con arresto domiciliario nocturno, como sería la obligación de permanecer en casa todos los días entre las 21:00 horas y las 7:00 horas del día siguiente, cabe preguntarse con qué fin se mantiene vigilado al sujeto el resto del día. Por otro lado, si lo que existe es una orden de alejamiento ¿para qué se consignarían los datos de la actividad física del portador del brazalete?

Incluso la información relativa a la ubicación de una persona sobre el planeta puede tornarse desproporcionada respecto de los fines que se persiguen, lo que trae como consecuencia que el Estado debe realizar los ajustes pertinentes para reducir los datos personales al mínimo necesario, pues los métodos electrónicos de vigilancia inciden en el retroceso o merma de los derechos fundamentales como la identidad, la libertad de asociación, de reunión, de práctica de convicciones religiosas y, sobre todo, de dignidad.

En cuanto a la revisión del efectivo cumplimiento del principio de calidad, esta nos lleva a cuestionarnos cuánto tiempo puede conservar el Estado los datos transmitidos por estos dispositivos: ¿un mes, un año, a perpetuidad?

En general, la idea que debe prevalecer es que una vez que se hayan cumplido las penas que dieron origen a la sanción, los datos obtenidos deberían ser anulados o bien convertidos en información anónima.

Sobre el deber o principio de transparencia, cabe señalar que los dispositivos telemáticos tienen que ser permitidos por ley, pues imponen restricciones de derechos constitucionales (algunos de ellos de carácter fundamental). Lo anterior implica que el Estado debe procurar a las personas toda la información que sea necesaria para garantizar y vigilar el adecuado tratamiento de los datos personales, a la vez que se delimitan los grados de responsabilidad entre los diferentes intervinientes en el proceso de su tratamiento, estableciendo mecanismos concretos que permitan corregir situaciones fuera de la

ley y todo lo relativo al ejercicio efectivo de los derechos de acceso, rectificación, oposición y cancelación, que es la manera de verificar la vigencia de estos principios.

9.3 Internet de las cosas (IoT) y tratamientode datos personales

Uno de los soportes fundamentales de la cuarta Revolución Industrial es la amplia expansión de las tecnologías de internet de las cosas (conocida como IoT por su acrónimo en inglés: *Internet of Things*), las que crecientemente ocupan parte importante del uso de la red internet, a través de la transmisión de datos que emanan de sensores ubicados en objetos, como relojes inteligentes, marcapasos y dispositivos médicos, ropa, dispositivos de realidad aumentada y un largo etcétera que aumenta día a día y que, incluso, abarca infraestructura pública como puentes, medición de caudales de agua y controles de señalética vial. Como nos dice Moisés Barrio Andrés:

"El método técnico es la incorporación de capacidades inteligentes a todos estos objetos tradicionalmente pasivos (o 'tontos'), a través de dispositivos hardware específicos (o simplemente de sensores inalámbricos), a fin de que puedan recopilar datos para su envío a centros de procesamiento por medio de una estructura de red interconectada".[154]

Ello tiene una importante arista procesal, pues si los datos viajan desde los sensores a los centros de procesamiento es legítimo preguntarse en qué momento y cómo nos hacemos de ellos, de forma de tener certeza no solo de que no ha sido alterado su contenido durante el tránsito de los mismos, sino también respecto de a quién se los vamos a requerir, pues "las pruebas, cualquier que sea su naturaleza, material o personal, pueden verse expuestas, por el mero transcurso del tiempo o por la propia decisión de la contraparte o de terceros, a mutaciones o cambios que pueden frustrar su práctica o influir en su fiabilidad".[155]

154 BARRIO ANDRÉS, Moisés: "Internet de la cosas. Desafíos jurídicos en un mundo de la conectividad total". En *Nuevas tecnologías y derecho*, al cuidado de María Yolanda Sánchez-Urán Azaña y María Amparo Grau Ruiz, Juruá, Oporto, 2019; p. 33.

155 ASENCIO MELLADO, José María: *Derecho procesal civil*, 3ª ed., Tirant lo Blanch, Valencia, 2015; p. 247.

Pero, apartado ese punto, debe tenerse claro que los aparatos IoT en sí, cualquiera de ellos, está constituido por un *sensor* que mide diferentes tipos de variables (temperatura, ubicación geográfica, presión, humedad, etcétera); un *actuador*, cuyo accionamiento activa procesos que producen cambios en el mundo físico (suelen ser neumáticos, hidráulicos o eléctricos), y un *controlador*, que gestiona el software, hardware, redes de comunicaciones electrónicas y demás tecnologías presentes en el dispositivo para que, ante la ocurrencia de determinadas variables, el *actuador* funcione o deje de hacerlo.[156]

Se trata de un conjunto de objetos físicos imbuidos de múltiples tecnologías, conectados a la red internet a través de protocolos de comunicaciones, y que tienen capacidades de interacción con el entorno, las cuales van desde la simple observación y registros de datos hasta la intervención en la realidad.

La influencia y el alcance de este tipo de invenciones han llegado a tanto, que la propia Unión Internacional de Telecomunicaciones (UIT) se ha ocupado de definir lo que entiende por internet de las cosas, señalando que es una "infraestructura mundial para la sociedad de la información que propicia la prestación de servicios avanzados mediante la interconexión de objetos (físicos y virtuales) gracias a la interoperatividad de tecnologías de la información y la comunicación presentes y futuras"[157]; pero esta definición no es la única que existe[158], y probablemente tenga el sesgo propio del área a la que se dedica la UIT, por ello centra la cuestión en el hecho de ser una infraestructura de comunicaciones, pero no necesariamente es este su aspecto más relevante.

En términos generales, se trata de un conjunto de objetos físicos imbuidos de múltiples tecnologías, conectados a la red internet a través de protocolos de comunicaciones, y que tienen capacidades de interacción con el entorno, las cuales van desde la simple observación y registros de datos hasta la intervención en la realidad. En

156 Las explicaciones están basadas en lo expuesto por BARRIO ANDRÉS, Moisés: *Internet de las cosas*, Reus, Madrid, 2018; p. 36.

157 UNIÓN INTERNACIONAL DE TELECOMUNICACIONES. *Descripción general de Internet de los objetos. Recomendación UIT-T Y.2060*, Ginebra, 2014; p. 6.

158 Si hacemos caso de Yakubuv-Trembach, no deberíamos fascinarnos con las definiciones, pues "Internet de las Cosas es un concepto evolutivo y no estático, según el Centro Criptológico Nacional, que lo define tanto por su parte física y conectividad, cosas que perciben, actúan y se comunican (artefactos, vehículos, edificios, electrodomésticos, atuendos, o implantes), como por sus funcionalidades e interdependencias entre sus componentes, las comunicaciones y las plataformas". Ver YAKUBUV-TREMBACH, Andreu: "20 años de internet de las cosas: retos arrastrados para la privacidad y otros derechos fundamentales", en *Era Digital, Sociedad y Derecho*, al cuidado de Olga Fuentes Soriano, Tirant lo Blanch, Valencia, 2020; p. 234.

otras palabras, son objetos que se conectan con otros y, en función de sus características técnicas, esa conexión se refleja en el comportamiento o funcionamiento de otros objetos.

No se trata de una idea nueva, según nos recuerda López i Seuba[159], pues los seres humanos siempre hemos creado aparatos que hacen *algo* o que se activan frente a ciertos estímulos predeterminados: los relojes de nuestra infancia golpeaban unas campanillas cuando llegaba la hora de levantarse, y todavía hay teteras o hervidores de agua que *silban* cuando el agua que contienen alcanza el punto de ebullición.

Incluso, un caricaturista e ingeniero norteamericano alcanzó la celebridad diseñando elaborados mecanismos de reacción en cadena en los que, deliberadamente, se utilizaban muchos recursos para alcanzar resultados de extraordinaria simpleza, dando lugar a lo que en su honor se han denominado "Máquinas de Rube Goldberg" (una esfera metálica golpea fichas de dominó, las que caen y golpean un automóvil de juguete que cae por una canaleta, etcétera).

Pero a diferencia de los ejemplos anteriores, los dispositivos de internet de las cosas pueden ayudar a realizar operaciones extraordinariamente complejas como, usando el mismo ejemplo de López y Seuba, regar un campo de trigo determinando por sí mismo, qué zonas regar, cuándo hacerlo y por cuánto tiempo, además de regular los flujos de agua teniendo a la vista los parámetros necesarios para obtener una cosecha óptima.

El uso de IoT no tiene ya nada de acotado o experimental, sino que se está usando masivamente en los medios de producción de las industrias, en la gestión *inteligente* de las ciudades y en el día a día de la vida las personas, siendo utilizado incluso en dispositivos de soporte vital de algunas de ellas.

159 LÓPEZ I SEUBA, Manel: *Internet de las cosas. La transformación digital de la sociedad*, Ra-Ma, Madrid, 2019; pp. 25-26.

A estas alturas, existen muchas definiciones de lo que es internet de las cosas, cada una de ellas formuladas desde distintos campos o áreas del conocimiento o con determinada orientación profesional; de hecho, ya presentamos una.

Sin embargo, desde el punto de vista de la naturaleza jurídica de los dispositivos de IoT, es del todo relevante la definición establecida por el desaparecido Grupo de Trabajo del Artículo 29[160], hoy reconvertido en el Comité Europeo de Protección de Datos[161], el cual definió internet de las cosas (al que se refirieron como "internet de los objetos", IO), como "una infraestructura en la que miles de millones de sensores incorporados a dispositivos comunes y cotidianos ('objetos' como tales, u objetos vinculados a otros objetos o individuos) registran, someten a tratamiento, almacenan y transfieren datos y, al estar asociados a identificadores únicos, interactúan con otros dispositivos o sistemas haciendo uso de sus capacidades de conexión en red".[162]

Esta definición es diferente a la que hemos visto con anterioridad, pues en lo medular se centra en la actividad de tratamiento de datos, esto es, en "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión,

160 El Grupo de Trabajo sobre Protección de Datos del Artículo 29 estaba compuesto por un representante de la autoridad de protección de datos de cada Estado miembro de la Unión Europea, el Supervisor Europeo de Protección de Datos y la Comisión Europea. Su nombre y estatuto proviene del artículo 29 de la 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 respeta al tratamiento de datos personales y a la libre circulación de estos datos; fue lanzado en 1996 y funcionó hasta el 25 de mayo de 2018, cuando entró a regir el Reglamento General de Protección de Datos. El nombre Reglamento no debe llamar a error, pues no se trata de potestades normativas del Poder Ejecutivo de cada país, sino que en la nomenclatura del Derecho Comunitario europeo los Reglamentos son actos legislativos vinculantes que deben aplicarse en su integridad en toda la Unión Europea, es decir, rigen directamente dentro de los países de la Unión, a diferencia de las Directivas, que son actos legislativos en los cuales se establecen objetivos que todos los países deben cumplir, pero donde le corresponde a cada uno de ellos elaborar sus propias leyes para alcanzar dichos objetivos.

161 El Comité Europeo de Protección de Datos (CEPD) es un organismo europeo independiente que contribuye a la aplicación coherente de las normas de protección de datos en toda la Unión Europea y también promueve la cooperación entre las autoridades de protección de datos de la Unión Europea. El CEPD se creó mediante el Reglamento General de Protección de Datos y tiene su sede en Bruselas.

162 Dictamen 8/2014 sobre la evolución reciente de la Internet de los Objetos, del Grupo de Trabajo sobre Protección de Datos del Artículo 29, adoptado el 16 de septiembre de 2014.

difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción"[163], así como también pone el acento en la capacidad de conexión de estos datos a redes de comunicaciones electrónicas, actividades que realizan tanto las personas físicas, como las organizaciones empresariales, municipios, organizaciones de nivel local y, por cierto, el conjunto de los organismos del Estado.

Las tecnologías IoT, más que los aspectos físicos como el hardware o el software que lo hace operar, son tecnologías que generan datos y en la medida que dichos datos sean atribuibles a una persona determinada o determinable, su tratamiento estará sujeto a la Ley Nº 19.628.

Debemos tener presente que por el solo hecho de ser objeto de tratamiento los datos de una persona física, ello trae consigo una serie de implicancias constitucionales, usualmente relacionadas con la intimidad, la vida privada, el derecho a la propia imagen o directamente el derecho constitucional a la protección de datos en los países que lo han incorporado a su Carta Fundamental[164]; a lo que debe sumarse las regulaciones legales existentes a lo largo de todo el orbe, todas cuestiones que hay que tener a la vista a la hora de obtener los datos capturados por un objeto con tecnologías IoT.

Y en lo que nos ocupa, la conclusión es que las tecnologías IoT, más que los aspectos físicos como el hardware o el software que lo hace operar, son tecnologías que generan datos y en la medida que dichos datos sean atribuibles a una persona determinada o determinable, su tratamiento estará sujeto a la Ley Nº 19.628.

163 Artículo 4.2 del Reglamento (UE) 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 y por el que se deroga la Directiva 95/46/CE, conocido internacionalmente como Reglamento General de Protección de Datos (RGPD).

164 Es el caso de países como Suecia, Portugal, Eslovaquia, Eslovenia, Hungría, Polonia y Chile.

9.4 Videovigilancia e imágenes como datos personales

Desde siempre se ha sabido que videos e imágenes, en la medida que muestren datos de personas identificadas o identificables, están sujetos a las leyes sobre protección de datos personales.

Sin embargo, la creación y popularización de drones equipados con cámaras, así como globos con idéntica funcionalidad, ha potenciado hasta límites insospechados el rol de estos en la obtención, deseada o no, de información de carácter personal. Ello, en razón de que en operaciones como la inspección de infraestructuras, levantamientos topográficos, inspecciones agrícolas u otros servicios de fotografía y video, existe el riesgo de que se produzca la captura de datos personales en forma inadvertida.

También existen operaciones de videovigilancia en que derechamente se persigue tal fin, y aquí la aplicación de la Ley Nº 19.628 es indubitada, sin perjuicio de que la Corte Suprema ha establecido ciertos criterios (ajenos al texto legal, dicho sea de paso) al conocer el caso de la instalación de globos de vigilancia equipados con cámaras de seguridad, contratados por las comunas de Lo Barnechea y Las Condes de la ciudad de Santiago.[165]

En dicha ocasión, junto con reconocer que tales dispositivos son capaces de atentar contra el derecho a la vida privada y a la inviolabilidad del hogar, la Corte señala que "no cabe sino aceptar que quienes habitan en su radio de acción puedan sentirse observados y controlados, induciéndolos a cambiar ciertos hábitos o de inhibirse de determinados comportamientos dentro de un ámbito de privacidad como es la vida doméstica".

165 Sentencia de la Corte Suprema, rol N° 18.481–2016, de 1 de junio de 2016.

Luego, construye desde la nada un "régimen de autorización", cuyos elementos basales son: la delimitación de los espacios físicos que pueden ser grabados (espacios públicos y, excepcionalmente, los espacios privados abiertos cuando se esté haciendo el seguimiento de un posible delito); que un inspector o delegado municipal certifique, al menos una vez al mes, que no se hayan captado imágenes desde espacios de naturaleza privada, como el interior de viviendas, de establecimientos comerciales o de servicios, jardines, patios o balcones; la destrucción de las grabaciones innecesarias en un plazo de 30 días y, finalmente, señalando que todo ciudadano tendrá derecho de acceso a las grabaciones, estableciendo un pequeño y singular procedimiento de *habeas data* al efecto.

9.5 Datos en internet y redes sociales

No es de extrañar que en una sociedad red como la que habitamos, en la que sus miembros se comunican e interactúan entre sí a través de plataformas informáticas que interrelacionan flujos de datos, el tema de la protección de datos personales sea especialmente crítico.

Partamos por recordar que, desde el momento mismo en que una persona se registra en una red social como Facebook, Instagram, Twitter u otra, debe entregar sus datos personales aceptando, de paso, una serie de condiciones respecto del uso de los mismos.

A partir de ese momento, las plataformas van asociando la información, música, imágenes, textos y videos que los usuarios van subiendo a la red social, vinculándolos a los datos que les proporcionaron al momento de registrarse, así como también la información adicional que proporciona su entorno de interacción social a través de la propia red.

Como resultado, construyen un perfil muy preciso de las personas y esa información se transa en el mercado: la persona es el producto, lo que no significa que aun teniendo el consentimiento del titular de los datos, la red social deba cumplir con los estándares de confidencialidad y seguridad y seguridad de la información, adaptando su funcionamiento a la a la normativa de protección de datos vigente en el país que opera.

A continuación, reseñaremos parte de la jurisprudencia de la Excma. Corte Suprema en relación a este tema.

Rol/procedimiento	Doctrina
Nº 138.566-2020 (1.12.2020) **Apelación en recurso de protección**	La publicación de una fotografía extraída de la cuenta personal de Instagram del afectado asociada a la mención "acoso-abuso sexual", que se pone a disposición de terceros, sin su consentimiento, es un acto arbitrario e ilegal, que conculca el derecho constitucional del actor previsto en el artículo 19 Nº 4 de la CPR, al afectar la protección que se le debe a su vida privada y a su honra.

Nº 132.263-2020 (30.12.2020) **Apelación en recurso de protección**	Que (…) la libertad de expresión no tiene un carácter absoluto y, por cierto, se encuentra limitada por el derecho al buen nombre que le asiste al afectado por las expresiones deshonrosas que se han vertido en una red social pública, cuestión improcedente, toda vez que, con posterioridad, es el mismo recurrido el que realizó la denuncia que le franquea el ordenamiento jurídico, reconociendo que es a través de las vías ordinarias que se debe dilucidar si efectivamente aquél había incurrido en conductas contrarias a la ley (Considerando 11). Que, en consecuencia, solo cabe concluir que las expresiones vertidas por la recurrida, por medio de una red social, sin otorgar una posibilidad de respuesta o contra argumentación de la contraria, no pueden tener por objeto sino afectar la honra de quien es sindicado como autor del uso indebido de un vehículo municipal, cuestión que en el caso concreto se verifica, toda vez que las expresiones vertidas importan un menoscabo a la persona del actor y, además, la exhibición de su domicilio, una intromisión indebida en el ámbito de su intimidad (Considerando 13).
27.759-2019, 31.03-2020 **Apelación en recurso de protección**	Que (…) resulta posible colegir que el derecho a la honra del recurrente, consagrado en el artículo 19 N° 4 de la Constitución Política de la República, ha sido perturbado con las publicaciones objeto de la presente acción, toda vez que lo tildan de estafador y de persona que imparte cursos "chantas" y "mulas", expresiones que lo denuestan públicamente; actuar que por lo mismo es ilegal y arbitrario por carecer de razonabilidad, toda vez que la libertad de emitir opinión que asiste al recurrido no supone un ejercicio ilimitado e irrestricto de tal derecho en términos que le permita atribuir públicamente al actor un actuar reñido con la ley y poco profesional (Considerando 7º).

ACADEMIA JUDICIAL CHILE

SERIE DE DOCUMENTOS MATERIALES DOCENTES