Un sistema fragmentado: La protección sectorial de los datos personales en Chile

A fragmented system: Sectoral protection of personal data in Chile

Pablo Contreras[1] - Pablo Trigo[2] - Leonardo Ortiz[3]

RESUMEN / ABSTRACT

El texto analiza el modelo de protección de datos personales ante la ausencia de una autoridad de control. Se examina cómo se protegen los datos personales en sector público y en el sector privado. El artículo concluye que, a pesar de la inexistencia de una autoridad de control especializada, la garantía del derecho se da a través de competencias fragmentadas y sectoriales, en función de la agenda de cada entidad pública.

The paper analyzes the model of personal data protection in the absence of a supervisory authority. We examine how personal data is protected in the public and in the private sector. The paper concludes that, despite the non-existence of a specialized control authority, the guarantee of the right is given through fragmented and sectorial competences, depending on the agenda of each public entity.

[1] Profesor asociado de la Universidad Central de Chile, Santiago, Chile. Doctor en Derecho (SJD), Northwestern University. Correo electrónico: pablo.contreras@ucentral.cl. Dirección postal: Lord Cochrane 417, Santiago, Chile. http://orcid.org/0000-0002-1131-182X.
Este trabajo es parte de la investigación financiada por Fondecyt Regular N° 1200362, del cual es coinvestigador. Agradezco el apoyo de la Fundación Carolina por la beca de estancia posdoctoral en la Universidad de Valencia.

[2] Investigador doctoral, Vrije Universiteit Brussel (VUB), Law Science Technology & Society (LSTS) Research Group. Investigador asociado del Centro de Estudios en Derecho Informático (CEDI) de la Universidad de Chile. Magister Legum (LL.M.) en Derecho Internacional por la Universidad de Heidelberg y la Universidad de Chile. Correo electrónico: ptrigokr@vub.ac.be. Dirección postal: Pleinlaan 2, Room 4C339, 1050 Elsene, Bruselas, Bélgica.
Agradezco el apoyo de la Agencia Nacional de Investigación y Desarrollo (ANID) y su beca de doctorado en el extranjero, Beca Chile, en transformación digital y revolución tecnológica, convocatoria 2020, folio N° 720210011.

[3] Abogado. Licenciado en Ciencias Jurídicas y Sociales, Universidad Alberto Hurtado. Postítulo en Ciberseguridad, Universidad de Chile. Profesor de la Facultad de Derecho de la Universidad Alberto Hurtado. Correo electrónico: lortizmesias@gmail.com. Dirección postal: Almirante Barroso 10, Santiago, Chile. https://orcid.org/0000-0003-3753-4519.

Artículo recibido el 4 de enero de 2022 y aceptado el 10 de junio de 2022.

Palabras clave: Protección de datos personales, autoridad de control independientes, Servicio Nacional del Consumidor, Superintendencia de Salud, Comisión para el Mercado Financiero.

Keywords: Personal data protection, independent supervisory authorities, Chilean consumer protection agency, Chilean Health Superintendence, Chilean Financial Trade Commission.

Introducción

En Chile, el esquema regulatorio del derecho a la protección de datos personales descansa sobre una norma de carácter constitucional, contenida en el artículo 19 Nº 4 de la Carta Fundamental, que prescribe que el tratamiento y protección de los datos personales "se efectuará en la forma y condiciones que determine la ley". La formulación literal de este derecho fundamental –junto con sacrificar "densidad normativa", al no ahondar en el contenido constitucionalmente protegido– no hace alusión a la existencia de un órgano público especializado, encargado de garantizar o tutelar el ejercicio de los "derechos propios de la autodeterminación informativa"[4].

A nivel legal, esta omisión se mantiene, de tal forma que el ecosistema chileno de protección de datos personales se caracteriza -y distingue respecto de otros modelos comparados- por la ausencia de un "mecanismo de heterocontrol" de tipo administrativo, que en doctrina se denomina "autoridad de control"[5], a cargo de la supervisión y cumplimiento de su marco regulatorio general, a saber, la Ley Nº 19.628, sobre protección de la vida privada (en adelante "LPDP"). Para estos efectos, la autoridad de control puede ser entendida como:

> el órgano público de carácter unipersonal o pluripersonal autónomo que, de forma imparcial e independiente, ejerce sus potestades y funciones para supervisar el cumplimiento de la normatividad de protección de datos personales con el fin de proteger los derechos y libertades fundamentales de las personas sobre el tratamiento de sus datos personales[6].

Señala Cerda que el propósito de esta instancia administrativa es:

> informar los derechos de los ciudadanos frente al tratamiento automatizado de datos que les conciernen, asesorar a los responsables de tratamiento, visar los códigos de conducta adoptados por entidades públicas o privadas, fiscalizar el cumplimiento de la legislación y sancionar las infracciones cometidas respecto de ella o abogar por que así ocurra, según sea el caso[7].

[4] Contreras 2020, 115.

[5] Cerda 2012, 36.

[6] Davara Fernández de Marcos 2019, 87.

[7] Cerda 2012, 37.

La inexistencia de una autoridad de este tipo ha sido denunciada de forma unánime por la doctrina nacional[8]. Como ha señalado Viollier, en términos generales, el hecho que no exista una autoridad de control:

> implica que los individuos afectados deben recurrir ante los tribunales ordinarios de justicia, sea a través de la acción constitucional de protección, o a través de las vías establecidas en la ley para hacer efectivos sus derechos y resguardarse del tratamiento de datos por parte de terceros[9].

Este modelo judicial de tutela ha sido criticado pues pone la carga en el titular de datos personales, con los costos y demoras que ello conlleva[10], con escasa jurisprudencia relevante sobre la legalidad de diversos tratamientos de datos[11] y por carecer de sanciones adecuadas para la ejecución de la ley[12].

Asimismo, es parte de las principales observaciones que, en su momento, hizo el Departamento de Evaluación de la Ley de la Cámara de Diputados, en su diagnóstico respecto de la LPDP[13]. En efecto, tal como se consigna en su informe:

> [l]a ausencia de un organismo que eduque, controle y fiscalice la protección de datos personales con un alcance transversal a todos los actores que tratan información de estas características, es indicada como una de las principales debilidades de la norma en Evaluación[14].

Pese a que la LPDP tiene más de 20 años –y que desde hace más de diez se ha intentado por todos los gobiernos conducir una reforma que dote de una institucionalidad especializada en la materia[15]–, al día de hoy continuamos con la inexistencia de una autoridad de control encargada de la supervisión y cumplimiento de las reglas sobre tratamiento y protección de datos personales.

La ausencia de una autoridad de control hace impracticable el *enforcement* independiente que se requiere en esta materia. Además, impide la supervisión especializada de la legislación de protección de datos personales. Sin embargo, del hecho que no exista una agencia especializada e independiente no significa que las materias relativas a la protección de datos personales queden sin supervisión alguna. En este trabajo argumentaremos que la inexistencia de una agencia tal ha generado la irrupción sectorial y fragmentada de distintas instituciones que empiezan a regular o fiscalizar a

[8] González Hoch 2001; Arrieta 2009; Camacho 2014; Álvarez 2016; Viollier 2017; Álvarez 2020.

[9] Viollier 2017, 26-27.

[10] González Hoch 2001, 177.

[11] Álvarez 2016, 52-54.

[12] Arrieta 2009, 18; Camacho 2014, 81; Viollier 2017, 47; Álvarez 2020, 1.

[13] Cámara de Diputados 2016.

[14] Cámara de Diputados 2016, 84.

[15] Viollier 2017, 28 y ss.

sus sujetos obligados en asuntos típicamente considerados sobre la protección de datos personales[16].

En particular, estimamos que el sistema de protección de datos personales en Chile está siendo descentralizadamente administrado por los órganos cuyas competencias entran en el radio de asuntos de datos personales. Para ello, es conveniente separar la esfera pública de la Administración respecto de la esfera privada de particulares. Esta distinción se hace con fines meramente ilustrativos, pues permite visualizar el tipo de instituciones que intervienen en una y otra esfera, sin prejuzgar sobre los casos de grises o frontera. Así, esta revisión provee la oportunidad de dibujar el archipiélago del control y supervisión en materia de protección de datos personales, a través de múltiples agencias con distintas potestades y competencias.

El trabajo se estructura de la siguiente forma. En el ámbito público, el *enforcement* está radicado principalmente en entes que controlan la Administración: el Consejo para la Transparencia y la Contraloría General de la República (II). Respecto de los particulares, la fragmentación es sectorial y el regulador de turno es quien tiene las atribuciones de control, en ocasiones, con reglas especiales en materia de datos personales. En este trabajo examinamos tres agencias para ejemplificar el tipo de control y supervisión posible, con las competencias que la ley les brinda. En primer término, se analiza el caso del Servicio Nacional del Consumidor, las reglas aplicables y cómo han evolucionado sus competencias en esta materia (III). Luego se revisa el caso de la Superintendencia de Salud, con el objeto de ejemplificar cómo este tipo de instituciones –las superintendencias– tienen un rol residual en la protección de datos personales en las materias de su competencia (IV). Por último, se indaga en la Comisión para el Mercado Financiero, como un ejemplo de agencia que supera el criticado modelo de las superintendencias (V). Estas instituciones permiten delinear el fragmentado mapa del control y *enforcement* de la protección de datos personales en Chile, teniendo especialmente presente el universo de sujetos sometidos a su función de supervisión y la relevancia que las operaciones de tratamiento de esta clase de información tienen para el desarrollo de las actividades sujetas a su función regulatoria y/o de fiscalización, pudiendo comprender datos amparados por un estatuto reforzado de protección (datos sensibles) o datos sometidos a reglas más estrictas para su comunicación a terceros (datos patrimoniales negativos)

El trabajo concluye que la ausencia de una autoridad de supervisión del derecho a la protección de los datos personales constituye un determinante clave del referido proceso de fragmentación regulatoria, y que se caracteriza por la existencia de distintos organismos públicos que, en el ámbito de su competencia y sobre la base de sus atribuciones genéricas, han venido a regular –con mayor o menor extensión– diversos aspectos relacionados con la

[16] El problema de la fragmentación regulatoria aparece también en otros ámbitos relacionados con la protección de los datos personales, por ejemplo, en materia de seguridad de la información. Véase Yuraszeck 2021.

tutela de los sujetos titulares de datos personales o con los deberes que recaen sobre las entidades responsables de las bases de datos. Este escenario no solo incide en la adecuada ponderación de este derecho fundamental respecto de otros derechos o bienes jurídicos, sino que también en su ejercicio y efectiva tutela.

II. La fragmentación de competencias respecto de los organismos públicos

1. Consejo para la Transparencia

Por el lado de la Administración, existen dos órganos relevantes: el Consejo para la Transparencia (CPLT) y la Contraloría General de la República (CGR). El primero tiene una atribución expresa en su ley, cual es, la de "[v]elar por el adecuado cumplimiento de la ley N° 19.628, de protección de datos de carácter personal, por parte de los órganos de la Administración del Estado" (art. 33, letra m) de la Ley N° 20.285). Se trata de una competencia a la que se le ha prestado escasa atención desde la doctrina, con las excepciones de Jijena[17] y Álvarez[18]. Para el primer autor, en un informe en derecho preparado para el Consejo para la Transparencia, sostuvo que el art. 33 letra m) tiene el siguiente efecto:

> [e]n el hecho y en Derecho, el Consejo para la Transparencia se ha constituido con esta facultad genérica y amplia en una entidad pública y autónoma que debe fiscalizar el respeto de todas las normas técnicas y jurídicas relacionadas con la gestión diligente de los sistemas de tratamiento de datos personales o nominativos en el sector público o al interior de la Administración del Estado[19].

En base a lo anterior, Jijena sostiene que el Consejo para la Transparencia puede fiscalizar a los órganos de la Administración en el cumplimiento de las disposiciones sobre tratamiento de datos personales, requerir información pertinente, inspeccionar las bases de datos personales y dictar instrucciones de carácter general o particular respecto de las condiciones de legitimidad de un tratamiento de datos personales, pero en el entendido que "sería una función meramente informativa y que no podría sancionarse si no se cumpliera con lo instruido"[20].

Posteriormente, en 2013, el autor ha agregado que la atribución del Consejo supone que la "competencia de vigilancia o tutela se extiende a la definición que se haga de las políticas de privacidad respecto de los datos

[17] Jijena 2009 y 2013.

[18] Álvarez 2016.

[19] Jijena 2009, 184.

[20] Jijena 2009, 187. El autor descarta que el Consejo pueda mantener un registro único nacional de bases de datos, requerir la inscripción de los bancos de datos que no estén registrados conforme al art. 22 de la Ley N° 19.628, conocer de las reclamaciones de *habeas data* y ejercer potestades sancionadoras contra los responsables de tratamiento de datos personales en la Administración. Véase Jijena 2009, 187-188; Jijena 2013, 69 y 87 y ss.

personales de los ciudadanos disponibles, accesados, recopilados y registrados mediante los sitios web de los servicios públicos"[21]. Pese a lo anterior, Jijena cambia –o matiza– su criterio original de 2009 relativo a la facultad de instruir, aunque sea meramente en términos informativos. En efecto, en su opinión, afirma que el art., 33, letra m):

> [n]o es, de modo alguno, un mandato abierto para 'instruir' ahora bajo la denominación de 'recomendación', reglamentar y establecer nuevos requisitos no contemplados en el texto de la Ley 19.628, crear procedimientos de reclamo de habeas data ilegales, y autoasignarse competencia para conocer alternativamente de los recursos del artículo 12 de la Ley 19.628, lo que nunca estuvo ni en el espíritu ni en el debate del legislador de la Ley 20.285[22].

Álvarez, por otro lado, ha analizado tangencialmente esta atribución a partir de su revisión más amplia sobre si el Consejo puede ser la autoridad de control de protección de datos personales en Chile[23]. Constata que el Consejo publicó una serie de recomendaciones en materia de tratamiento de datos personales por parte de los órganos de la Administración del Estado[24] y que ha debido aplicar directamente la LPDP en casos de amparos o reclamos por acceso a la información[25]. No obstante, en lo relativo al alcance de la citada atribución, Álvarez afirma que:

> esta resulta insuficiente para constituir al CPLT como autoridad de control por cuanto su campo de acción se encuentra reducido a los órganos de la Administración del Estado, careciendo de competencias específicas sobre los privados que realizan algún tipo de tratamiento de datos personales[26].

Es decir, para Álvarez, el hecho que el Consejo contemple una atribución exclusiva respecto de los órganos de la Administración impide que sea considerado una autoridad de control, propiamente tal, de cara al estándar internacional.

Para finalizar la revisión de las competencias del Consejo y sus competencias en materia de protección de datos personales. Como ha quedado claro de la revisión de la literatura, la atribución solo cubre a la Administración y no comprende potestades sancionadoras. La facultad fiscalizadora, sin embargo, no está en cuestionamiento. En efecto, tal como dictaminó la Contraloría General de la República:

---

[21] Jijena 2013, 60.
[22] Jijena 2013, 88.
[23] Álvarez 2016.
[24] Álvarez 2016, 61.
[25] Álvarez 2016, 66.
[26] Álvarez 2016, 70, n/p 60.

> la ley junto con conferir al Consejo para la Transparencia atribuciones para fiscalizar el cumplimiento de la Ley de Transparencia, le encomienda expresamente la función de velar por la reserva de los datos personales por parte de los órganos de la Administración del Estado y por el cumplimiento de la ley N° 19.628, para lo cual lo habilita para recabar toda la información necesaria al efecto[27].

Ello incluye actividades de auditoría y la "instrucción de procedimientos tendientes a la obtención de la información que requiera", puesto que el Consejo puede "decidir sobre los medios o instrumentos idóneos" para el fin de velar por la reserva de los datos personales de la LPDP, respecto de los órganos de la Administración[28].

2. Contraloría General de la República

Además del Consejo para la Transparencia, la Contraloría General de la República (CGR) opera como un mecanismo de control a través de sus atribuciones tradicionales, cuando se trate de órganos de la Administración como responsables del tratamiento y los deberes de los funcionarios públicos relacionados. En efecto, solo durante el 2020, la CGR ha emitido cuatro importantes dictámenes circunscribiendo las competencias de los servicios públicos con relación a la legalidad del tratamiento de datos sensibles[29]. Además de su facultad dictaminadora, CGR revisa la legalidad ex ante de los actos de la Administración y, en dicha función, se ha pronunciado en casos emblemáticos de protección de datos personales, como el denominado "Decreto Espía"[30]. El Decreto N° 866 de 2017, del Ministerio del Interior y Seguridad Pública tenía por objeto reglar la interceptación de comunicaciones privadas, desbordando el marco legal establecido en el artículo 222 del Código Procesal Penal, motivando la representación del acto administrativo. Por último, y como es evidente, la CGR puede instruir los sumarios administrativos correspondientes por infracciones de funcionarios públicos a la LPDP. Esto demuestra que, a diferencia del Consejo para la Transparencia, la CGR si tiene una potestad para reprochar infracciones a la ley, a través del régimen disciplinario de la administración.

Para cerrar este apartado, cabe destacar que la fragmentación del sistema y las competencias parceladas impide que exista una tutela especializada de la protección de datos personales fuera de la administración, esto es, res-

---

[27] Dictamen N° 021167-19 (2019).

[28] Dictamen N° 021167-19 (2019).

[29] Sobre el acceso de los municipios a la ficha clínica de pacientes, véase Dictamen N° 008113-20 (2020); sobre el acceso de personal de ambulancias SAMU a identificación biométrica de pacientes por huella dactilar, véase Dictamen N° 009545-20 (2020); sobre la declaración de salud de funcionarios del Servicio Médico Legal para ejercer labores presenciales durante la pandemia, véase Dictamen N° 37912-20 (2020); y, finalmente, sobre las facultades del Servicio de Registro Civil y de Identificación para impedir el acceso a datos de terceros, véase Dictamen N° 30041-20 (2020).

[30] Dictamen N° 041188-17 (2017). Véase Viollier y Canales 2018.

pecto de otros poderes del Estado o respecto de los órganos constitucionalmente autónomos.

III. Consumo, derechos y datos personales: el caso del Servicio Nacional del Consumidor

En el ámbito privado, un supervisor de la protección de datos personales en las relaciones de consumo ha sido el Servicio Nacional del Consumidor (SERNAC), ahora confirmado por vía legislativa. SERNAC es un servicio encargado de velar por el cumplimiento de la Ley N° 19.496 ("LPDC") y "las demás normas que digan relación con el consumidor" (art. 58, inc. 1° LPDC). Si bien SERNAC carece de potestades sancionatorias –por decisión del Tribunal Constitucional[31]–, sí participa en el monitoreo de mercados, a través de su plan de fiscalización, y en términos generales, a través de distintas facultades.

Con la última reforma a la LPDC, SERNAC puede ejercer sus atribuciones, en materia de protección de datos personales, cuando estamos ante una relación de consumo. En enero de 2019, el Presidente de la República ingresó un proyecto de ley que establece medidas para incentivar la protección de los derechos de los consumidores (boletín N° 12.409-03, en adelante "PDL")[32]. El proyecto fue aprobado, promulgado y publicado como la Ley N° 21.398, que establece medidas para incentivar la protección de los derechos de los consumidores. Conforme a lo dispuesto por dicha ley, el nuevo art. 15 bis LPDC dispone lo siguiente:

> Las disposiciones contenidas en los artículos 2 bis letra b), 58 y 58 bis de la presente ley, serán aplicables respecto de los datos personales de los consumidores, en el marco de las relaciones de consumo, salvo que las facultades contenidas en dichos artículos se encuentren en el ámbito de competencias legales de otro órgano.

En esta sección se explica el problema normativo anterior respecto de las competencias del SERNAC, al que responde el art. 15 bis, y cómo esta regla configura amplias atribuciones en la materia.

1. El marco de protección de datos personales en la legislación de consumo, antes de la introducción del art. 15 bis LPDC

Reglas sobre protección de datos personales se encuentran en diversas disposiciones generales de la LPDC. En primer lugar, están las obligaciones de seguridad en el consumo. El art. 3, letra d) establece que son derechos básicos del consumidor "[l]a seguridad en el consumo de bienes o servicios, la protección de la salud y el medio ambiente y el deber de evitar los riesgos

[31] Sentencia TC Rol N° 4012-17 (2018). Sobre el debate generado, véase Contreras 2018.

[32] https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=12940&prmBOLETIN=12409-03.

que puedan afectarles". Este derecho tiene un correlato de obligaciones para el proveedor. Conforme al art. 23 de la LPDC:

> [c]omete infracción el proveedor que, en la venta de un bien o en la prestación de un servicio, actuando con negligencia, causa menoscabo al consumidor debido a fallas o deficiencias en la calidad, cantidad, identidad, sustancia, procedencia, seguridad, peso o medida del respectivo bien o servicio.

Dicha seguridad se extiende a la protección de datos personales en el marco de la relación de consumo[33].

Desde el punto de vista del *enforcement*, SERNAC ha ejercido distintas facultades, aún antes del art. 15 bis LPDC. Una revisión de algunos de los casos puede permitir determinar con mayor claridad las facultades del SERNAC en aplicación de estas reglas. Un primer caso lo constituye el denominado "cartolazo" del Banco de Chile, en donde la entidad bancaria envió por error cartolas de cuentas corrientes de sus clientes a terceros[34]. En base a ello, SERNAC ofició a la institución para que informara "a los consumidores quién tuvo acceso a sus datos personales y que se tomen los resguardos necesarios para que no se haga mal uso de ellos"[35]. Esta intervención terminó en un acuerdo extrajudicial donde la empresa se comprometió a contratar una póliza de seguro para todos los consumidores afectados, entregar un abono de $20.000 por las molestias de más de 50.000 afectados, un aumento de las medidas de seguridad de la información y un plan de ejecución en el plazo de 30 días[36].

En materia de cláusulas abusivas, la Corte Suprema ha fallado dos casos relativos a la protección de datos de los consumidores, de manera contradictoria[37]. La contradicción, además, explica en buena medida la motivación de parte de los colegisladores a reformar la LPDC, como se revisa en el siguiente apartado.

En el primer caso, *SERNAC con Ticketmaster*[38], la Corte Suprema estimó que la cláusula de la política de privacidad del sitio web del proveedor era abusiva. Entre otras razones, declaró que la cláusula contenía:

---

[33] Adicionalmente, se puede citar el art. 15 de la Ley N° 19.406, que establece que los "sistemas de seguridad y vigilancia que, en conformidad a las leyes que los regulan, mantengan los establecimientos comerciales están especialmente obligados a respetar la dignidad y derechos de las personas". Entre los "derechos de las personas" se puede entender comprendido, sin problemas, el derecho constitucional a la protección de datos personales, establecido en el artículo 19 N° 4 de la Constitución.

[34] SERNAC 2012a.

[35] SERNAC 2012a.

[36] SERNAC 2012b.

[37] Momberg 2017a; Momberg 2017b.

[38] *Servicio Nacional del Consumidor con Ticketmaster Chile S.A.* (2016).

> diversas autorizaciones a Ticketmaster. No son sin embargo autorizaciones que el usuario dé positiva y especialmente. Tampoco son autorizaciones supletorias que el usuario pueda denegar si así lo desea. Son autorizaciones que se entienden concedidas por el consumidor por el solo hecho de usar el sitio[39].

En este caso, la Corte asume que la Ley N° 19.496 era aplicable[40] y que la protección de datos personales de sus titulares podía ser defendido a través de la tutela de los intereses colectivos de los consumidores. En cierta forma, depende del fundamento desarrollado, con posterioridad, en *SERNAC con Créditos Organización y Finanzas S.A.*[41], en donde revisó, precisamente, el alcance de la aplicación de la LPDP con relación a la LPDC. Frente a la alegación que la defensa de los datos personales supone un interés individual y personal de cada titular, la Corte Suprema afirmó lo siguiente:

> si bien el tratamiento de datos personales está regulado en una ley especial, la afectación de intereses supraindividuales que implica la contratación en situación de desigualdad mediante contratos de adhesión cuyo contenido acarrea el desequilibrio entre las partes que se refleja, entre otros, en el quebrantamiento de los derechos de los titulares de datos de carácter personal, constituye una materia susceptible de ser conocida en esta sede. Más clara es esta inferencia cuando se advierte que el proceso judicial de la ley de protección a la vida privada está previsto únicamente para el resguardo de un interés individual, mientras que el de estos antecedentes se refiere al interés colectivo de todos aquellos deudores que suscribieron el informativo convenio con la expectativa no cumplida de ser eliminados del Boletín Comercial, de manera que nos encontramos en el caso previsto en la letra b) del artículo 2 bis de la ley 19.496, ya que si bien las normas de protección al consumidor no son aplicables, en principio, en materia de datos personales, sí lo son cuando se compromete el interés colectivo o difuso[42].

No obstante, en *SERNAC con Ticketek*, la Corte negó a SERNAC la legitimación activa para obrar en la defensa de los datos personales de los consumidores[43]. A diferencia de lo resuelto en *Tickemaster* y *Créditos Organización y Finanzas S.A.*, la Corte entendió que la LPDP regula "una cuestión esencialmente individual", dado por la protección de la tenencia y uso de los datos personales y, en consecuencia, tiene un "procedimiento que nace del interés individual, que inicialmente se manifiesta en el requerimiento hecho al poseedor de los datos y que no necesariamente derivará en un pleito de carácter judicial"[44]. En consecuencia, concluye la Corte:

---

[39] *Servicio Nacional del Consumidor con Ticketmaster Chile S.A.* (2016), c. 11°.

[40] Momberg 2017a, 361.

[41] *Servicio Nacional del Consumidor con Créditos Organización y Finanzas S.A.* (2016).

[42] *Servicio Nacional del Consumidor con Créditos Organización y Finanzas S.A.* (2016).

[43] *Servicio Nacional del Consumidor con Ticketek Co. SpA* (2016).

[44] *Servicio Nacional del Consumidor con Ticketek Co. SpA* (2016), c. 6°.

> no es posible asumir que la ley especial pueda ceder ante la general, aún en el caso de procedimientos de interés colectivo o difuso de los consumidores, puesto que la naturaleza de los asuntos regulados por la Ley 19.628 es esencialmente individual, sin que tengan cabida los procesos colectivos[45].

La respuesta legislativa apunta, precisamente, al corazón de la sentencia de la Corte Suprema en el caso *Ticketek*. La reforma a la LPDC afirma, explícitamente, que las normas jurídicas sobre protección de datos personales, contenidas en la LPDP, son normas jurídicas especiales a la luz de la LPDC. Estos alcances se explican a continuación.

2. La reforma a la LPDC y las obligaciones expresas en materia de protección de datos personales

a) El origen del art. 15 bis LPDC

El art. 15 bis es una norma de origen peculiar. No estaba prevista en el mensaje original del Presidente de la República y su base fue una regla incorporada y aprobada en el segundo trámite constitucional por el Senado. Sin embargo, dicha disposición fue rechazada en tercer trámite constitucional y fue la única norma en desacuerdo sometida a la revisión de la Comisión Mixta del PDL. En esta instancia, el debate giró sobre las competencias del SERNAC como autoridad de control en materia de protección de datos personales[46]. Entre las críticas al articulado propuesta se mencionaba "un debilitamiento del derecho [a la protección de datos personales]"[47], que el SERNAC no es una autoridad independiente y que ello no permitiría que Chile fuese reconocido por la Unión Europea como un país que brinda un nivel adecuado de protección de datos personales[48], que el proyecto generaría una "falsa sensación de resolución de los problemas que aquejan a la ciudadanía"[49] y que es una respuesta legislativa "cortoplacista"[50] que puede tener como consecuencia el retraso de la modificación integral de la LPDC.

Pese a las críticas, la Comisión mixta aprobó una regla que eliminó en su totalidad lo aprobado inicialmente por la Cámara –en materia de deberes de seguridad– y dejó establecidas las competencias para el SERNAC en materia de protección de datos personales. El alcance de la disposición se explica a continuación.

b) El contenido del art. 15 bis LPDC

El art. 15 bis de la LPDC consta de un inciso:

---

[45] *Servicio Nacional del Consumidor con Ticketek Co. SpA* (2016), c. 6°.

[46] El debate público giró precisamente en torno a este aspecto. Véase Contreras 2021.

[47] Matus 2021.

[48] Pessó 2021.

[49] Zaror 2021.

[50] Diario Financiero 2021.

> [l]as disposiciones contenidas en los artículos 2 bis letra b), 58 y 58 bis de la presente ley, serán aplicables respecto de los datos personales de los consumidores, en el marco de las relaciones de consumo, salvo que las facultades contenidas en dichos artículos se encuentren en el ámbito de competencias legales de otro órgano.

La disposición en comento presenta las siguientes características:

a) Es una regla especial de competencia del SERNAC, que clarifica cuáles atribuciones puede ejercer respecto del tratamiento de datos personales de consumidores.

b) El ámbito de aplicación de la regla de competencia se circunscribe a "los datos personales de los consumidores, en el marco de las relaciones de consumo". Habría que entender que las competencias seleccionadas por el legislador se refieren a los tratamientos de datos personales que efectúan los proveedores en el marco de la relación de consumo. Por lo tanto, no es una competencia general del SERNAC respecto a la protección de datos personales, en tanto derecho fundamental aplicable a todas las dimensiones de la vida de una persona natural. Es una protección circunscrita a la relación de consumo, esto es, la relación entre proveedores y consumidores, en los términos del art. 1° LPDC.

c) Conforme a la disposición, el SERNAC tiene las siguientes competencias. En primer término, la facultad de iniciar procedimientos colectivos y el derecho a solicitar la indemnización a través de éstos (art. 2 bis, letra b) LPDC). En segundo lugar, se aplican todas las funciones y atribuciones del SERNAC, contenidas en el art. 58 LPDC, cuya extensión amerita un desarrollo adicional. Tercero, SERNAC tiene a su cargo el registro de sentencias con información referente a las causas iniciadas por infracción de la LPDC (art. 58 bis LPDC).

d) El artículo 58 LPDC establece catorce funciones y atribuciones de SERNAC, todas las que son aplicables en materia de protección de datos respecto de relaciones de consumo. No es necesario reproducir su contenido. Salvo por las potestades sancionatorias que fueron declaradas inconstitucionales, en su oportunidad, el SERNAC tiene amplísimas competencias para fiscalizar, interpretar la legislación, efectuar propuestas normativas, iniciar procedimientos voluntarios colectivos, denunciar incumplimientos a la ley, generar programas de educación, realizar estudios en el área de consumo, publicar información sobre características de comercialización de bienes y servicios, entre otras. La letra g) del art. 58 establece una función general: "[v]elar por el cumplimiento de las disposiciones legales y reglamentarias relacionadas con la protección de los derechos de los consumidores […]".

Esto implica, por ejemplo, que el SERNAC puede fiscalizar a un proveedor sobre las bases de licitud para el tratamiento de datos de sus clientes, revisar los estándares de seguridad de la información, verificar la información a que tiene derecho el titular de datos y cómo han respondido las solicitudes

de los titulares de datos, cumpliendo con la LPDP respecto de consumidores. Pero además puede dictar una circular interpretativa, realizar promoción y educación sobre la protección de datos respecto de la ciudadanía, en general, o denunciar los incumplimientos de la ley ante los tribunales de justicia cuando se infrinja la LPDP por parte de un proveedor.

Sin abarcar todas las dimensiones de la vida de una persona, el art. 15 bis LPDC alcanza un importante número de interacciones de los titulares de datos. Evidentemente, el mayor responsable del tratamiento de datos personales queda fuera: el Estado. Sin perjuicio de ello, esta reforma ha modificado considerablemente el modelo de *enforcement* de protección de datos personales en el sector privado –y, específicamente, en la relación entre consumidores y proveedores.

e) Con una confusa técnica legislativa, estas tres competencias generales no serán aplicables cuando "se encuentren en el ámbito de competencias legales de otro órgano". Esta parte del enunciado pretende resolver el problema de concurrencia de competencias ante la creación de una eventual autoridad de control independiente en materia de protección de datos personales. Sin embargo, no es claro cómo debe interpretarse o cómo podría coordinarse con otra agencia. Estas serán algunas de las dudas que los tribunales deberán despejar, especialmente, si se llegare a crear una autoridad de control en materia de protección de datos personales.

IV. El modelo de las superintendencias: el caso de la Superintendencia de Salud

El segundo tipo de instituciones que tiene a cargo una protección sectorial de datos personales corresponde a las superintendencias. Sin perjuicio de los aspectos de diseño institucional anotados por la literatura[51], estas instituciones ejercen de hecho, un rol residual relevante en el modelo de *enforcement* sectorial del derecho de protección de datos personales, en razón de las materias propias de su competencia. Así, dependiendo de su regulación orgánica-sectorial, cuentan con atribuciones directas en la materia, ya sea porque explícitamente se establecen a su respecto atribuciones de fiscalización[52]; o indirectas, porque con motivo de sus funciones y atribuciones fiscalizan a entidades que en virtud de sus cometidos, tratan datos personales y/o sensibles[53]. Con fines ilustrativos, analizaremos el caso de la Superintendencia de Salud ("Superintendencia"). Lo anterior, sin perjuicio del análisis sectorial que

[51] Véase, Galetovic y Sanhueza 2002; García 2009; García y Verdugo 2010; Díaz de Valdés 2010; Cordero y García 2012.

[52] Esto ocurre en el caso de la Superintendencia de Salud, como veremos.

[53] Así, por ejemplo, ocurre con la Superintendencia de Telecomunicaciones respecto de los servicios de telecomunicaciones (art. 7 inc. final de la Ley N° 18.168 General de Telecomunicaciones); o la Superintendencia de Educación, respecto de establecimientos educacionales (art. 49, letra o) de la Ley N° 20.529 que crea el Sistema Nacional de Aseguramiento de la Calidad de la Educación Parvularia, Básica y Media y su fiscalización).

pudiere efectuarse respecto del resto de entidades que componen el esquema de superintendencias cuyas competencias se superpongan con aspectos de protección de datos personales.

La Superintendencia es garante del derecho a la protección de datos personales, por parte de usuarios del sistema sanitario en aquellos temas que, en el ámbito de sus competencias, ejerce potestades generales y especiales de supervigilancia y control respecto de los distintos sujetos pasivos involucrados, tales como Instituciones de Salud Previsional (Isapres), Fondo Nacional de Salud (Fonasa), prestadores de salud, ya sean públicos o privados, entre otros. En lo medular, dos son las fuentes normativas a partir del cual se configura el esquema de facultades en la materia: aquellas contenidas en el Decreto con Fuerza de Ley N° 1 del Ministerio de Salud, de 2006, que fija el texto refundido, coordinado y sistematizado del decreto ley N° 2.763 de 1979 y de las leyes N° 18.933 y N° 18.469 (en adelante, "DFL N° 1 Minsal"); así como aquellas contenidas en la Ley N° 20.584, de 2012, que regula los derechos y deberes que tienen las personas en relación con acciones vinculadas a su atención en salud, a propósito del deber de confidencialidad de fichas clínicas.

1. Protección de datos personales en virtud del DFL Nº 1 del Minsal del año 2006

El DFL N° 1 Minsal es el principal instrumento normativo que otorga a la Superintendencia potestades fiscalizadoras y sancionatorias en materia de protección de datos personales. Se trata de una regulación dispuesta por la Ley N° 20.635 de 2012, que adecúa dicha normativa general a la Ley N° 20.575, de 2012, que establece el principio de finalidad en el tratamiento de datos personales. Las atribuciones sectoriales de control y supervigilancia encomendadas a la Superintendencia en la materia, se traducen en la de un mandato general de licitud en el tratamiento de datos personales, así como en la prohibición específica de los sujetos pasivos de fiscalización en el ámbito sanitario (Isapres, Fonasa y prestadores de salud) de consultar información comercial de usuarios, pacientes o beneficiarios. Las describiremos en lo que sigue.

a) Mandato general de licitud en el tratamiento de datos sensibles de usuarios, beneficiarios o pacientes

El mandato general de protección de datos personales encomendado a la Superintendencia tiene como destinatario, a todo prestador de salud, Isapre, Fonasa u otras entidades, tanto públicas como privadas, que elaboren, procesen o almacenen datos de origen sanitario, imponiéndoseles la prohibición de "vender, ceder o transferir, a cualquier título, bases de datos que contengan información sensible respecto de sus usuarios, beneficiarios o pacientes, sino cuentan para ello con el consentimiento del titular de tales datos", de conformidad a la LPDP u otras normas especiales que regulen la materia (art. 134 bis DFL N° 1 Minsal). Dicha norma, exime de la obligación de consenti-

miento, cuando la información sea destinada al "otorgamiento de los beneficios de salud que correspondan, así como del cumplimiento de sus objetivos legales […]". (art. 134 bis DFL N° 1 Minsal).

Este deber general de licitud en el tratamiento de datos personales a cargo de la supervigilancia de la Superintendencia, tiene como contrapartida, un régimen sancionatorio especial en esta materia, y que está previsto por las reglas contenidas en el artículo 121 N° 11 del DFL N° 1 Minsal. De conformidad a dicha regla (la que fue incorporada por la Ley N° 20.635), se establece explícitamente la potestad de la Superintendencia de fiscalizar y sancionar a los prestadores de salud en las infracciones cometidas de conformidad a lo dispuesto en los artículos 134 bis; 141, incisos penúltimo y final; 141 bis; 173, incisos séptimo y octavo, y 173 bis. De esta manera, las infracciones al deber general de licitud en el tratamiento de datos personales por parte de entes fiscalizados, pueden ser sancionadas, en atención a su gravedad, con una multa de 10 y hasta 1000 UTM. Tratándose de *prestadores institucionales*, además de la multa, se les eliminará del registro nacional y regional de prestadores institucionales acreditados (art. 121 N° 5 DFL N° Minsal). Tratándose de *prestadores individuales*, junto a la multa serán sancionados, si correspondiere, con suspensión de hasta 180 días para otorgar las Garantías Explícitas en Salud (GES), sea por medio de Fonasa o Isapre, así como para otorgar prestaciones en la modalidad de libre elección de Fonasa. Con todo, en el caso de reincidencia dentro del período de 12 meses contado desde la comisión de la primera infracción, se aplicará una multa desde 2 hasta 4 veces el monto de la multa aplicada por dicha infracción.

En razón del contenido de este mandato general de licitud en el tratamiento de datos personales por parte de agentes de salud, se trata de un reenvío general y expreso al dispuesto por la LPDP. Sin embargo, atendida la falta de una agencia de control especializada en materia de protección de datos personales, así como el débil régimen sancionatorio dispuesto por la legislación general, el régimen sectorial sancionatorio dispuesto por el DFL N° 1 Minsal goza de un mejor estándar ante eventuales infracciones en el ámbito sanitario.

b) Prohibición especial de Isapres, Fonasa y prestadores de salud de consultar información comercial de usuarios, pacientes o beneficiarios

En lo que a información comercial respecta, el DFL N° 1 Minsal prohíbe a Isapres, Fonasa y prestadores de salud consultar sistemas de información comercial de ningún tipo, ni aun con el consentimiento del paciente, para efectos de condicionar o restringir una atención de urgencia (arts. 141 inc. final y 173 inc. 8°). La infracción a esta prohibición especial de comunicación de datos comerciales es sancionada de conformidad al régimen sancionatorio general previsto por el artículo 121 N° 11 del DFL N° 1 Minsal.

La prohibición de *consulta* de información comercial por agentes de salud vendría a configurar una especie de contrapartida a la obligación de cier-

tas entidades responsables de registros o bancos de datos personales de *no comunicar* información comercial a terceros por la LPDP (art. 17). A este respecto, llama la atención que el DFL Nº 1 Minsal regule únicamente la prohibición de consulta y no la prohibición de comunicación de deudas contraídas en el ámbito de la salud a terceros, como es el diseño regulatorio de la LPDP. Desde la otra vereda, también es llamativo que la LPDP regule la prohibición de deudas contraídas con empresas públicas o privadas que presten servicios de electricidad, agua, teléfono, gas y educación, pero relegue la regulación de información comercial con ocasión de prestación de servicios sanitarios a un ámbito sectorial con competencias de *enforcement* bien delimitadas.

La disparidad regulatoria advertida deja en evidencia la fragmentación del control del sistema de protección de datos personales en el sector sanitario. Se trata de obligaciones o prohibiciones que, atendido su contenido, bien podrían ser susceptibles de tener un respaldo bajo el ámbito de aplicación de la LPDP. Sin embargo, atendida las deficiencias ampliamente conocidas de dicho régimen legal general, una disposición sectorial como la advertida tiene efectos positivos sólidos con miras a evitar discriminaciones arbitrarias o diferencias de trato respecto del acceso a cuidado sanitario en desmedro de usuarios.

2. Protección de datos personales y ficha clínica

Un tema relevante respecto del cual la Superintendencia ejerce control y supervigilancia, dice relación con el deber de reserva de la información contenida en la ficha clínica, el que está regulado en los arts. 12 y 13 de la Ley Nº 20.584, que regula los derechos y deberes que tienen las personas en relación con acciones vinculadas a su atención en salud. Esta ley, encomienda a la Superintendencia de Salud, a través de su Intendencia de Prestadores, controlar su cumplimiento por los prestadores de salud públicos y privados, recomendando la adopción de medidas necesarias para corregir las irregularidades que se detecten. En caso de no ser corregidas dentro del plazo previsto por dicha ley, la Superintendencia tiene la facultad de aplicar los procedimientos y las sanciones establecidas mediante el régimen general de fiscalización y sanción contemplado en el DFL Nº 1 Minsal (art. 38 Ley Nº 20.584). En este sentido, la Ley Nº 20.584 efectúa un reenvío normativo a dicho régimen procedimental-sancionatorio, entre cuyas reglas se encuentran, precisamente, las contenidas en el artículo 121 Nº 11 del DFL Nº 1 Minsal (que fue incorporada por la Ley Nº 20.635) en materia de protección de datos personales en el ámbito sanitario.

En relación al régimen de protección de la ficha clínica, cabe preguntarse si a pesar de las facultades otorgadas a la Superintendencia en este ámbito, es susceptible de ser aplicado el régimen general de protección de datos personales contemplado por la legislación. La regulación de la confidencialidad o acceso a la ficha clínica de conformidad al régimen general de protección de datos personales brindado por la LPDP no ha sido un tema pacífico en la doctrina. Para Donoso, "queda claro que los datos contenidos en

una receta médica, en un examen médico y en la ficha médica son claramente datos sensibles"[54]. Sin embargo, Eterovic lo controvierte: a su juicio, tal interpretación tiene consecuencias jurídicas importantes, pues, entre otras, "posicionaría al paciente con un derecho preferente sobre el médico en lo relativo al ejercicio de derechos sobre la ficha clínica"[55], esto es, los derechos de acceso, rectificación, cancelación y oposición, que no son afines a los propósitos de dicho instrumento de salud. Para fundar su posición, Eterovic indica que la LPDP estaría enfocada a tratar los datos recopilados en "bases de datos", lo que a su juicio, es muy distinto a la labor realizada por el médico respecto de las fichas; que la historia fidedigna de la LPDP muestra que ésta emergió para regular datos de carácter financiero o comercial y de aquellos contenidos en registros, bases de datos y ficheros, condicionando su ámbito de aplicación y protección a su incorporación en tales soportes; o que la única categoría de datos sensibles que reconocería la LPDP en el ámbito de salud, son las recetas y exámenes médicos, la que debería ser interpretado restrictivamente[56].

De lo expuesto, aparece que las razones entregadas por Eterovic para no considerar a las fichas clínicas dentro del ámbito de regulación general de la LPDP permitirían situarla como una institución de protección *sui generis*. El problema de dicha tesis es el texto expreso de la Ley N° 20.584. En efecto, junto con otorgar una definición legal de "ficha clínica", la ley establece que aquella podrá configurarse de manera electrónica, en papel o en cualquier otro soporte, "siempre que los registros sean completos y se asegure el oportuno acceso, conservación y confidencialidad de los datos, así como la autenticidad de su contenido y de los cambios efectuados en ella" (art. 12 inc. 1° Ley N° 20.584). Más aún, la ley efectúa un reenvío expreso a la letra g) del artículo 2° LPDP, al considerar que "[t]oda la información que surja, tanto de la ficha clínica como de los estudios y demás documentos donde se registren procedimientos y tratamientos a los que fueron sometidas las personas, será considerada como dato sensible" (art. 12 inc. 2° Ley N° 20.584).

Ante dicha regulación, Eterovic destaca que lo calificado como dato sensible sería toda información que *surge de* la ficha clínica y no aquella por sí misma, lo que implicaría "un trabajo profesional detrás", pues en ellas "hay mucha información que puede llegar a ser depurada según su utilidad"[57]. Se trata la discusión entonces, de si lo protegido por la Ley N° 20.584 es el continente (ficha clínica) o el contenido (datos sensibles). Sin embargo, el concepto de ficha clínica (entendido como continente), no dista sustancialmente del concepto de registro o banco de datos previsto por la LPDP (art. 2°, letra m), lo que no excluye su ámbito de protección general con ocasión del tratamiento de tales datos. Lo anterior, no implica desde luego la necesidad

[54] Donoso 2011, 85.
[55] Eterovic 2019, 61.
[56] Eterovic 2019, 62-68.
[57] Eterovic 2019, 69.

de su regulación bajo un estatuto especial y perfectible por parte de la Ley N° 20.584, que excluya explícitamente ciertos institutos de la LPDP incompatibles con los objetivos de la ficha clínica, como lo es por ejemplo, el libre y discrecional ejercicio de los derechos ARCO por parte de su titular.

Finalmente, tal como se indicó, el artículo 38 de la Ley N° 20.584 es claro al disponer que el agente de control respecto del acceso y confidencialidad de la ficha clínica es la Superintendencia de Salud, por intermedio de su Intendencia de Prestadores. La Corte Suprema ha tenido la oportunidad de pronunciarse sobre la entidad de control a cargo de la fiscalización de la ficha clínica en términos negativos, indicando que Fonasa carece de atribuciones de fiscalización[58] y sanción[59] a prestadores de salud en este ámbito.

V. El modelo de un nuevo regulador: el caso de la Comisión para el Mercado Financiero

1. Antecedentes

El último caso que revisamos corresponde a la Comisión para el Mercado Financiero (en adelante, "CMF" o "Comisión"). Esta institución fue creada por la Ley N° 21.000, viniendo a reemplazar, a la Superintendencia de Valores y Seguros. Este cambio tuvo por objeto introducir mejoras profundas a la institucionalidad de supervisión del mercado de valores y seguros, comprendiendo, entre otros aspectos, la modernización de su marco jurídico, el fortalecimiento de su gobierno corporativo (introduciendo un modelo colegiado) y el perfeccionamiento de su estructura orgánica[60], incorporando, además, el nuevo mandato legal de velar por el correcto funcionamiento, desarrollo y estabilidad del mercado financiero[61].

La principal función de la Comisión dice relación con "velar por el correcto funcionamiento, desarrollo y estabilidad del mercado financiero, facilitando la participación de los agentes de mercado y promoviendo el cuidado de la fe pública," así como "velar porque las personas o entidades fiscalizadas, desde su iniciación hasta el término de su liquidación, cumplan con las leyes, reglamentos, estatutos y otras disposiciones que las rijan". (artículo 1°, incisos segundo y tercero, de la Ley N° 21.000). Caben dentro del ámbito de fiscalización de la CMF, según dispone el artículo 3° del referido cuerpo legal, las personas que emitan o intermedien valores de oferta pública; las bolsas de valores mobiliarios; las operaciones bursátiles; las asociaciones de agentes de valores y las operaciones sobre valores que estos realicen; los fondos que la ley somete a su fiscalización y las sociedades que los administren; las sociedades anónimas y en comandita por acciones que la ley sujete a su vi-

[58] *Zuchel Matamala con Directora Zonal Centro Sur de Fonasa* (2020).

[59] *Vaccarezza con Fondo Nacional de Salud* (2021).

[60] Boletín N° 9015-05.

[61] Nacrur y Ried 2020, 64.

gilancia; las empresas dedicadas al comercio de asegurar y reasegurar, así como de las personas que intermedien seguros; el Comité de Autorregulación Financiera; y, cualquiera otra entidad o persona natural o jurídica que la Ley N° 21.000 u otras leyes le encomienden.

Dentro del ámbito de su competencia, la CMF puede ejercer potestades normativas e interpretativas. Dispone el numeral primero del artículo 5° de la Ley N° 21.000 que la Comisión puede "[d]ictar las normas para la aplicación y cumplimiento de las leyes y reglamentos y, en general, dictar cualquier otra normativa que de conformidad con la ley le corresponda para la regulación del mercado financiero". Asimismo, la Comisión tiene la función de "interpretar administrativamente las leyes, reglamentos y demás normas que rigen a las personas, entidades o actividades fiscalizadas, y podrá fijar normas, impartir instrucciones y dictar órdenes para su aplicación y cumplimiento". Por otra parte, y en el marco de sus atribuciones normativas, la CMF cuenta con la facultad de establecer reglas relacionadas con la información financiera de sus fiscalizados[62].

El 12 de enero de 2019, se publicó la Ley N° 21.130, que Moderniza la Legislación Bancaria, modificando el Decreto con Fuerza de Ley N° 3 de 1997, que fija texto refundido, sistematizado y concordado de la Ley General de Bancos (en adelante, indistintamente, "LGB"). La Ley N° 21.130 vino a generar una nueva institucionalidad regulatoria y modelo de supervisión del sector bancario y financiero, traspasando todas las competencias y facultades de la Superintendencia de Bancos e Instituciones Financieras a la Comisión para el Mercado Financiero. De esta forma, todas las instituciones fiscalizadas por dicha Superintendencia (v.gr. empresas bancarias, empresas cuyo giro consista en la emisión u operación de tarjetas de crédito, tarjetas de pago con provisión de fondos o de cualquier otro sistema similar a dichos medios de pago) quedaron sujetas a la supervisión de la CMF. Entre dichas competencias, destacan ciertas atribuciones específicas para dictar normas de carácter general aplicables a las operaciones realizadas por las entidades bancarias y financieras fiscalizadas por la Comisión.

2. La LPDP y los datos personales de carácter económico

Resulta indudable el rol fundamental que desempeñan las operaciones de tratamiento de información personal en los contextos financieros, en especial los datos personales patrimoniales, sean estos positivos (activos financieros) o negativos (pasivos financieros). El procesamiento de estos datos no solo resulta indispensable para la adecuada prestación de servicios bancarios o crediticios, sino que también para el resguardo de ciertos intereses públicos, tales como promover o asegurar la estabilidad financiera, principalmente a través de los sistemas de información sobre morosidades[63], o prevenir y de-

[62] Nacrur y Ried 2020, 82.

[63] Bozzo 2020, 102.

tectar fraudes[64]. Asimismo, cobran relevancia aspectos relacionados con la seguridad, integridad y confidencialidad de los sistemas o redes informáticas financieras.

Si bien la LPDP se refiere en particular, en su Título III, a los datos de contenido económico, financiero, bancario o comercial, lo cierto es que aborda solo algunos datos patrimoniales negativos –a saber, aquellos que dan cuenta de una obligación o deuda listada en el mismo Título III[65]– configurándolos como una "categoría intermedia" de datos, sujetos a hipótesis de comunicación más restrictivos[66].

Teniendo presente lo anterior, y considerando la ausencia de una autoridad de control en materia de protección de datos personales, dotada de la facultad de, a lo menos, interpretar el marco legal general, resulta relevante referirse, en primer lugar, a ciertas normas especiales aplicables al tratamiento de ciertos tipos de datos patrimoniales (tanto de tipo positivo como negativo) en los entornos bancarios y/o financieros, para, luego, abordar la labor normativa desplegada por la CMF en su rol de ente supervisor sectorial.

3. Normativa sectorial de relevancia en materia de tratamiento de datos personales

Respecto de las operaciones y sujetos comprendidos dentro del ámbito de competencia de la CMF, cabe destacar diversas normas, legales y administrativas, que tienen injerencia en las actividades de tratamiento de datos personales que tienen lugar en los mercados financieros, de valores y seguros.

a) Artículo 14, inciso segundo, de la Ley General de Bancos

El inciso segundo del artículo 14 de la LGB establece que:

> [c]on el objeto exclusivo de permitir una evaluación habitual de las instituciones fiscalizadas en virtud de la presente ley por firmas especializadas que demuestren un interés legítimo, la Comisión deberá darles a conocer la nómina de los deudores de las entidades antes señaladas, los saldos de sus obligaciones y las garantías que hayan constituido. Lo anterior solo procederá cuando la Comisión haya aprobado su inscripción en un registro especial que abrirá para los efectos contemplados en este inciso y en el inciso cuarto del artículo 154. La Comisión mantendrá también una información permanente y refundida sobre esta materia para el uso de las instituciones fiscalizadas en virtud de la presente ley. Las personas que obtengan esta información no podrán revelar su contenido a

[64] Mantelero 2015, 37.

[65] Jervis 2005, 125.

[66] Jara 2001, 70-72. Jervis los denomina como "datos patrimoniales negativos comunicables" (Jervis 2005, 133).

terceros y, si así lo hicieren, incurrirán en la pena de reclusión menor en sus grados mínimo a medio[67].

Esta norma legal da cuenta de una regla que habilita, bajo ciertos supuestos, determinadas operaciones de procesamiento y comunicación de datos financieros bancarios, concernientes a personas naturales identificadas. Específicamente, esta disposición ordena a la CMF la entrega a firmas especializadas que "demuestren un interés legítimo" –y que se encuentren inscritas en un registro especial elaborado por la Comisión–[68] de información sobre la nómina de los deudores de las entidades fiscalizadas en virtud de la LGB, los saldos de sus obligaciones y las obligaciones que hayan constituido. Asimismo, la Comisión debe mantener una "información permanente y refundida sobre la materia", denominado como "Estado de Deudores" y que se forma a partir de la información que las entidades financieras entregan a la CMF, la que puede ser utilizada exclusivamente por las mismas instituciones fiscalizadas. La entrega de esta información debe efectuarse de acuerdo a las instrucciones contenidas en el Capítulo 18-5 de la Recopilación Actualizada de Normas (en adelante, indistintamente, RAN) de la CMF,[6970] así como a lo dispuesto en el Manual del Sistema de Información referente al sistema de deudores.

b) Artículo 154 de la Ley General de Bancos

La LGB regula en su artículo 154 el secreto y la reserva bancaria, disponiendo en su inciso primero que:

[l]as operaciones de depósitos y captaciones de cualquier naturaleza que reciban los bancos en virtud de la presente ley estarán sujetas a secreto bancario y no podrán proporcionarse antecedentes relativos a dichas operaciones sino a su titular o a quien haya sido expresamente autorizado por él o a la persona que lo represente legalmente. El que infringiere la norma anterior será sancionado con la pena de reclusión menor en sus grados mínimo a medio.

A continuación, el inciso segundo de la citada norma agrega:

[l]as demás operaciones quedarán sujetas a reserva y los bancos en virtud de la presente ley solamente podrán darlas a conocer a quien

[67] Artículo 14 del D.F.L. N° 3, de 1997, del Ministerio de Hacienda, que fija el texto refundido, sistematizado y concordado de la Ley General de Bancos.

[68] Entidades evaluadoras de instituciones financieras (agencias clasificadoras de riesgo).

[69] Estas normas de origen administrativo tienen un "rango inferior a la ley y al reglamento", teniendo por objeto "regular extensivamente ciertas materias sujetas a la competencia normativa de las superintendencias". Díaz de Valdés 2020, 266 y ss.

[70] El Capítulo 18-5 de la RAN, relativo a información sobre deudores de las instituciones financieras, contiene reglas relativas, entre otros aspectos, a las operaciones de crédito que deben informarse y los importes adeudados; oportunidad y forma de entrega de la información; responsabilidad en la entrega de la información; y, manejo de la información por parte de las instituciones financieras.

demuestre un interés legítimo y siempre que no sea previsible que el conocimiento de los antecedentes pueda ocasionar un daño patrimonial al cliente[71].

Del tenor literal resulta claro que la regla sobre secreto y reserva bancaria, en vista a la amplitud de las operaciones que comprende, puede incluir información de índole patrimonial (tanto positiva como negativa) concerniente a clientes que revistan la calidad personas naturales identificadas o identificables.

c) Decreto Supremo N°950 del Ministerio de Hacienda de 1928

El Decreto Supremo Nº 950 de 1928 del Ministerio de Hacienda, entrega a la Cámara de Comercio de Santiago A.G. la labor de recopilar y sistematizar diversa información de carácter financiero, con el objeto de facilitar los procesos de evaluación crediticia y riesgo comercial. De esta forma, se procede a la elaboración y publicación de un banco de datos financiero, el Boletín de Informaciones Comerciales, que contiene la información indicada en el artículo 1° del referido Decreto Supremo Nº 950[72].

Esta base de datos incluye los protestos de letras de cambio y de pagarés practicados en las Notarías; los protestos de cheques efectuados por los bancos; las cuotas morosas 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, las aclaraciones de tales protestos y cuotas morosas, de modo de informar al mercado los pagos o regularizaciones de los incumplimientos comerciales por parte de los deudores publicados previamente en él[73].

d) Capítulo 20-10 de la Recopilación Actualizada de Normas (RAN)

El 1 de diciembre de 2020, entró en vigencia el nuevo Capítulo 20-10 de la RAN, con reglas para la gestión de la seguridad de la información y ciberseguridad[74]. Estas disposiciones –que son aplicables a bancos, filiales bancarias, sociedades de apoyo al giro bancario y emisores y operadores de tarjetas de pago– obedecen a la creciente de conectividad y dependencia de los servicios brindados a través de plataformas tecnológicas, teniendo por

[71] Artículo 154 del D.F.L. Nº 3, de 1997, del Ministerio de Hacienda, que fija el texto refundido, sistematizado y concordado de la Ley General de Bancos.

[72] Resultan igualmente aplicables las normas especiales contenidas en el Título III de la LPDC, sobre utilización de datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial, así como lo dispuesto en la Ley Nº 20.575, que establece el principio de finalidad en el tratamiento de datos personales.

[73] En el Capítulo 20-6 de la RAN, sobre publicación en el Boletín de Informaciones Comerciales, la CMF establece un conjunto de normas relativas al envío de información al BIC.

[74] Capítulo 20-10 de la Recopilación Actualizada de Normas, denominado "gestión de la seguridad de la información y ciberseguridad", cuyo contenido fue fijado por la Circular Nº 2.261 de la Comisión para el Mercado Financiero, de 6 julio de 2020

objeto, por una parte, asegurar la adecuada calidad y disponibilidad de estos sistema y, por la otra, hacer frente a la progresiva exposición a los riesgos asociados al uso de las tecnologías de la información y comunicación.

Concretamente, la norma aborda aspectos vinculados a la evaluación de la gestión de la seguridad de la información y ciberseguridad[75], así como la implementación de un adecuado proceso de gestión de riesgos; la realización de procesos de diligencia para determinar los activos críticos de ciberseguridad, junto con las funciones de protección de estos activos, la detección de las amenazas y vulnerabilidades, la respuesta ante incidentes y la recuperación de la operación normal de la entidad; y, la identificación de los activos que componen la infraestructura critica de la industria financiera y del sistema de pagos del país, así como el adecuado intercambio de información técnica de incidentes que afecten o pudieran afectar la ciberseguridad. Cabe destaca el hecho que el numeral 2 de referido capítulo menciona entre los elementos considerados como necesarios para un adecuado sistema de gestión de la seguridad de la información y ciberseguridad el "cumplimiento de las leyes y normativas vigentes, entre las que se encuentran, por ejemplo, la protección de los datos de carácter personal".

e) Capítulo 20-7 de la RAN

Las disposiciones del Capítulo 20-7 de la RAN, sobre externalización de servicios[76], permiten, cumpliendo algunos requisitos, la contratación por parte de las instituciones bancarias "de proveedores de servicios externos para que realicen una o más actividades operativas que podrían ser también efectuadas internamente por la entidad con sus propios recursos, tanto humanos como tecnológicos", incluyendo los servicios de procesamiento de datos[77].

El capítulo dispone que la entidad "debe cerciorarse que el proveedor de servicio mantiene un programa de seguridad de la información que le permita asegurar la confidencialidad, integridad, trazabilidad y disponibilidad de sus activos de información y la de sus clientes", además de "controlar y

[75] Según el numeral primero de este capítulo, se entiende por seguridad de la información el "conjunto de acciones para la preservación de la confidencialidad, integridad y disponibilidad de la información de la entidad". La ciberseguridad, por su parte, comprendería el "conjunto de acciones para la protección de la información presente en el ciberespacio y de la infraestructura que la soporta", y que tienen por finalidad "evitar o mitigar los efectos adversos de sus riesgos y amenazas inherentes, que puedan afectar la seguridad de la información y la continuidad del negocio de la institución".

[76] Capítulo 20-7 de la Recopilación Actualizada de Normas, denominado "externalización de servicios", cuyo contenido fue fijado por la Circular N° 3.570 de la Superintendencia de Bancos e Instituciones Financieras, de 7 de octubre de 2014.

[77] Según dispone el numeral 3 de la Circular N° 2 de la CMF, las empresas emisoras de tarjetas de pago no bancarias y las empresas operadoras de tarjetas de pago deben igualmente observar las instrucciones contenidas en el referido Capítulo 20-7, en lo que respecta, entre otros aspectos, a "[l]as condiciones que deben cumplirse en la externalización de servicios, a que se refiere el Título III", "[l]as consideraciones contenidas en el Título IV a excepción del numeral 2" y "[l]os requisitos considerados en el Título V".

monitorear la infraestructura de seguridad de la información dispuesta por el proveedor, con el objeto de proteger los activos de información presentes en los servicios críticos externalizados, independiente de los controles dispuestos por el proveedor" (Título III, N° 4). Por otra parte, se dispone que las "conexiones de comunicaciones entre la entidad contratante y el proveedor de servicios deben contar con un nivel de cifrado que asegure la confidencialidad y la integridad de los datos de punta a punta". Asimismo, una vez procesada la información, debe ser "almacenada y transportada en forma encriptada, manteniéndose las llaves de desencriptación en poder de la entidad".

Se impone, también, a las entidades bancarias el deber de comunicar a la CMF "los incidentes operacionales que afecten un servicio externalizado en el país o en el exterior", en los términos definidos en el Capítulo 20-8 de la RAN. Dicho capítulo contempla requisitos relativos a la información que se debe enviar a la CMF cuando ocurran incidentes que "afecten o pongan en riesgo la continuidad del negocio, los fondos o recursos de la entidad o de sus clientes, la calidad de los servicios o la imagen de la institución". Esta información debe enviarse a la CMF dentro del plazo máximo de 30 minutos luego de ocurrido el incidente[78].

Con las modificaciones introducidas a este capítulo por la Circular N° 2.244, de Bancos, de la CMF de fecha 23 de diciembre de 2019, los bancos pueden externalizar servicios en jurisdicciones que no cuenten con calificación de riesgo país en grado de inversión, "en la medida que el país en el que se externalizan los servicios cuente con leyes de protección y seguridad de datos personales adecuadas".

En el caso que la entidad bancaria externalice servicios de procesamiento de datos fuera del país, establece el Título IV del referido capítulo que se debe contar con un "Centro de Procesamiento de Datos de contingencia ubicado en Chile". Con todo, los bancos que mantengan una adecuada gestión del riesgo operacional pueden quedar exceptuados de este requerimiento, siempre que aseguren, por medio de un informe anual, que cumplen con la adopción de las ciertas "medidas preventivas"[79].

Cabe mencionar que, según dispone este capítulo de la RAN, cualquier operación que involucre el procesamiento de datos que se encuentren sujetos a reserva o secreto bancario de acuerdo con lo establecido en la LGB, constituye una actividad significativa o estratégica (críticas), lo que implica ciertos

[78] Asimismo, se establece la obligación de mantener adecuadamente informados a los clientes en determinados eventos y el deber de los bancos de compartir con el resto de la industria información de ataques relacionados a ciberseguridad.

[79] Estas medidas dicen relación con el tiempo de recuperación objetivo (RTO); el tiempo de disponibilidad de operación de los *sites* de procesamiento de datos; la ubicación de estos *sites*, con miras a mitigar tanto el riesgo geográfico como los riesgos políticos; y, que los servicios externalizados se provean en un ambiente consistente con las políticas y estándares adoptados por la entidad.

deberes de diligencia reforzados, por ejemplo, respecto a la contratación de servicios de *cloud computing*, en los términos señalados en su Título V.

f) Documento de Política: "Desarrollo de estándares y principios generales en materia de Conducta de Mercado referidos a Protección al Cliente Financiero"

Con fecha 24 de junio de 2021, la CMF publicó un documento con estándares y principios generales de Conducta de Mercado para la protección del cliente financiero. Si bien esta clase de documentos, "por su naturaleza, no constituyen una instrucción normativa ni una política de supervisión", dan cuenta de la "visión de la Comisión y su Consejo sobre temas relevantes para la industria financiera", pudiendo constituir una "guía del estándar o mejores prácticas esperadas por la CMF"[80].

La mencionada guía señala respeto al marco legal y regulatorio general aplicado en la CMF en conducta de mercado con foco en protección del cliente financiero, que "se han considerado regulaciones relativas a la mantención de diversos registros y a velar por la protección de los datos personales y privacidad de la información de los clientes". Luego, el documento identifica cinco principios de conducta de mercado para entidades financieras, el tercero de los cuales se refiere a específicamente a la "protección de la información de los clientes". A este respecto, se reconoce, en el contexto de los servicios financieros, la importancia de la seguridad de la información, al involucrar el tratamiento de una "cantidad significativa de antecedentes [...] de carácter financiero, médico y personal". Por consiguiente, la salvaguarda de estos datos financieros y personales "es una de las principales responsabilidades de la industria de servicios financieros".

Así, se hace expresa mención a la necesidad de dar cumplimiento al principio de licitud en el tratamiento de estos datos, junto con los principios de finalidad y proporcionalidad. De igual manera, se hace referencia al respeto de los derechos de información, acceso, rectificación y cancelación que asisten a los titulares de datos personales, junto con la posibilidad que éstos tienen de revocar el consentimiento inicialmente otorgado. Por otra parte, se hace mención al deber de "trasparentar e informar a los clientes sobre la política de tratamiento de datos de la entidad". Cabe advertir que el documento hace alusión, a partir del derecho de acceso, a un supuesto derecho a la portabilidad de los datos.

A continuación, se refiere con cierto detalle a los deberes de confidencialidad y de seguridad a los que se encuentran sujetas las entidades finan-

[80] Disponible en línea: https://www.cmfchile.cl/portal/prensa/615/w3-article-47838.html. Esta clase de documentos podrían ser considerados como instrumentos de *soft law*, que "sin ser obligatorios para los sujetos obligados, tienen por objeto explicitar los criterios o lineamiento de trabajo interno del órgano administrativo", junto con permitir conocer con anterioridad "la interpretación administrativa que realizará el ente en sus procesos de fiscalización del cumplimiento". Bravo 2020, 158.

cieras, abordando la necesidad de contar con medidas de protección tanto a nivel técnico como organizativo, incluyendo el desarrollo de "planes de contingencia que permitan mitigar los riesgos y el impacto de cualquier destrucción, alteración, filtración o uso indebido de la información".

Respecto a los tratamientos de datos efectuados a través de mandatarios, se dispone que se debe tener en cuenta "el riesgo que presenta la tercerización de actividades", debiendo verificarse que "las instituciones contratadas cuenten con adecuados mecanismos para resguardar la confidencialidad y seguridad de la información".

Finalmente, en cuanto al registro de deudas, el documento señala que las entidades deben brindar a los clientes "acceso fácil y gratuito a sus reportes y detallar los procedimientos a seguir para corregir errores".

Este documento viene a poner en relieve los esfuerzos de la CMF por abordar ciertos aspectos relevantes del procesamiento de datos en entornos financieros, sirviéndose de las categorías, principios, derechos y obligaciones propias del derecho a la protección de datos personales. Esta labor podría fundamentarse en el reconocimiento del derecho a la autodeterminación informativa como un derecho fundamental autónomo, cuyo contenido irradia a todo el ordenamiento jurídico, abarcando ciertamente la actividad normativa e interpretativa que ejercen los órganos de la administración.

En este sentido, cabe destacar que el ente supervisor no se circunscribe estos estándares a las reglas que establece expresamente la Ley N°19.628, sino que muestra una concepción del derecho a la protección de datos personales acorde con su desarrollo doctrinal y evolución a nivel comparado, lo que queda de manifiesto, por ejemplo, en la incorporación de deberes de transparencia, la adopción de un enfoque basado en riesgos y la referencia al derecho a la portabilidad de datos.

Conclusiones

En Chile, el esquema normativo en torno al derecho a la protección de los datos personales presenta altos grados de dispersión y fragmentación, situación que se agravada por la inexistencia de una autoridad de control en la materia.

Entendiendo que el modelo regulatorio que ampara a este derecho requiere construirse a partir del artículo 19 Nº 4 de la Constitución, se debe tener presente que dicha disposición –junto con omitir referirse a los principios mínimos que constituyen el núcleo del derecho a la protección de datos personales– no mandata la creación de un órgano público que, de manera comprehensiva, supervise o vele por este derecho. Asimismo, la LPDP carece de una autoridad de control que cuente con, al menos, la potestad de interpretar administrativamente sus disposiciones y de ejercer acciones de *enforcement*.

La falta de dicha autoridad constituye un catalizador clave del proceso de fragmentación regulatoria que afecta la autodeterminación informativa. En concreto, su garantía se deja a la suerte de competencias descentralizadamente ejecutadas por diversas instituciones, regulando o fiscalizando a sus sujetos obligados, respecto del tratamiento de datos personales que desarrollan.

Teniendo presente que el procesamiento de datos personales constituye un elemento imprescindible para el funcionamiento de diversos mercados o el ejercicio de la función pública de órganos estatales, las normas generales y sectoriales aplicables en dichas esferas han abordado –directa o indirectamente– múltiples aspectos concernientes a la protección de los datos personales. Así, se evidencia la intervención de distintos organismos encargados de supervisar de ciertos estatutos normativos, dictando –sobre la base de sus atribuciones genéricas– reglamentos, circulares e instrucciones que inciden en las actividades de procesamiento de datos personales, ya sea en cuanto a los derechos que asisten a los sujetos titulares de los mismos o en cuanto a las obligaciones que recaen sobre los responsables de las bases de datos, incluyendo requisitos técnicos aplicables a su gestión.

La ausencia de una autoridad de control especializada que vele por el cumplimiento de la LPDC conlleva diversas dificultades. En primer lugar, y desde un punto de vista cualitativo, la necesidad de garantizar el ejercicio legítimo de un derecho de las personas, más allá de su calidad de funcionario público, consumidor o paciente, entre otros. Segundo, se requiere operativizar este derecho siguiendo un conjunto de principios generales, entendidos a la luz de criterios uniformes, evitando de esta manera interpretaciones discordantes. Esta concentración competencial permite profundizar o dotar de contenido a los conceptos e instituciones propias de la autodeterminación informativa, por ejemplo, los procesos de anonimización o disociación de información, así como ciertos elementos técnicos propios de las actividades de tratamiento de datos personales, tales como los estándares mínimos que deben seguirse para el adecuado cumplimiento de los deberes de seguridad que recaen sobre los responsables de bases de datos. Finalmente, el derecho a la protección de datos personales puede verse afectado por la existencia de mecanismos de tutela o de sanción diversos, cuya aplicación dependerá del contexto dentro del cual se verifican las respectivas actividades de tratamiento (sea en cuanto a la naturaleza de la entidad responsable de la base de datos o del mercado específico dentro del cual se insertan las respectivas operaciones de procesamiento), lo que incide, en la práctica, en la existencia de estatutos de protección diferenciados y que pueden presentar disparidades en los niveles de resguardo de un mismo derecho fundamental.

Bibliografía citada

Álvarez Valenzuela, Daniel (2016). Acceso a la información pública y protección de datos personales. ¿Puede el Consejo para la Transparencia ser la autoridad de control en materia de protección de datos? *Revista de Derecho (Universidad Católica del Norte) 23*(1), 51-79.

Álvarez Valenzuela, Daniel (2020). Editorial: La protección de datos personales en contextos de pandemia y la constitucionalización del derecho a la autodeterminación informativa. *Revista Chilena de Derecho y Tecnología 9*(1), 1-4.

Arrieta, Raúl (2009). Chile y la Protección de Datos Personales. En Raúl Arrieta y Carlos Reusser (Coords.), *Chile y la Protección de Datos Personales* (pp. 13-22). Expansiva UDP.

Bravo Alliende, Felipe (2020). Medidas y sanciones de la Comisión para el Mercado Financiero. En Roberto Ríos (Coord.), *La Comisión para el Mercado Financiero* (pp. 145-194). Ediciones UC.

Bozzo Hauri, Sebastián. (2020). Sobreendeudamiento, sistemas de información crediticia y la protección de los datos personales del consumidor en Chile. *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso* (55), 99-130.

Camacho Cepeda, Gladys (2014). La Protección de Datos como Frontera del Derecho de Acceso a la Información en la Legislación Chilena. *Revista de Gestión Pública 3*(1), 73-93.

Cámara de Diputados (Agosto de 2016). *Evaluación de la Ley N° 19.628, Sobre Protección de la Vida Privada.* http://www.evaluaciondelaley.cl/wpcontent/uploads/2019/07/informe_final_ley_19628_con_portada.pdf.

Cerda Silva, Alberto (2003). Autodeterminación informativa y leyes sobre protección de datos. *Revista de Derecho Informático* (3), 47-75.

Cerda Silva, Alberto (2006). Mecanismos de control en la protección de datos en Europa. *Ius et Praxis 12*(2), 221-251.

Cerda Silva, Alberto (2012). *Legislación sobre Protección de las Personas frente al Tratamiento de Datos Personales.*

Contreras Vásquez, Pablo (15 de febrero de 2018). *Inconstitucionalidad de la reforma al SERNAC.* https://www.pcontreras.net/blog/inconstitucionalidad-de-la-reforma-al-sernac.

Contreras Vásquez, Pablo (2020). El derecho a la protección de datos personales y el reconocimiento de la autodeterminación informativa en la Constitución chilena. *Estudios constitucionales 18*(2), 87-120.

Contreras Vásquez, Pablo (7 de febrero de 2021). *Sernac y protección de datos personales.* https://www.pcontreras.net/blog/sernac-y-proteccion-de-datos-personales-compilacion-del-debate.

Cordero Vega, Luis y García, José Francisco (2012). Elementos para la discusión sobre agencias independientes en Chile. *Anuario de Derecho Público 2012*, 415-435.

Davara Fernández de Marcos, Isabel (Coord.) (2019). *Diccionario de protección de datos personales.* INAI.

Diario Financiero (30 de junio de 2021). Expertas enjuician el polémico artículo que entrega el Sernac facultades de protección de datos. *Diario Financiero*. https://www.df.cl/empresas/entre-codigos/expertas-enjuician-polemico-articulo-de-la-ley-del-consumidor-que

Díaz de Valdés Juliá, José Manuel (2010). Anomalías constitucionales de las superintendencias. *Estudios Constitucionales 8*(1), 249-282.

Donoso Abarca, Lorena (2011). El problema del tratamiento abusivo de los datos personales en salud. En VV.AA., *Reflexiones sobre el uso y abuso de los datos personales en Chile* (pp. 79-110). Expansiva.

Eterovic Barreda, Pablo (2019). *Acceso a la ficha clínica en el derecho chileno*. Ediciones Jurídicas de Santiago.

Galetovic, Alexander y Sanhueza, Ricardo (2002). Regulación de servicios públicos: ¿hacia dónde debemos ir? *Estudios Públicos* (85), 101-137.

García, José Francisco (2009). ¿Inflación de superintendencias? Un diagnóstico crítico desde el derecho regulatorio. *Revista de Actualidad Jurídica* (19), 327-371.

García, José Francisco y Verdugo, Sergio (2010). De las superintendencias a las agencias regulatorias independientes en Chile: Aspectos constitucionales y de diseño regulatorio. *Revista de Actualidad Jurídica* (22), Universidad del Desarrollo, 263-305.

González Hoch, Francisco (2001). Modelos comparados de protección de la información digital y la ley chilena de datos de carácter personal. *Cuadernos de Extensión Jurídica* (U. de los Andes (5), 153-178.

Jara Amigo, Rony (2001). Régimen de los datos de carácter económico financiero, bancario o comercial en la ley N°19.628". En Jorge Wahl Silva (editor), *La Ley chilena de Protección de Datos Personales: Una visión crítica desde el punto de vista de los intereses protegidos* (pp. 61-83). Ediciones Universidad de los Andes.

Jervis Ortiz, Paula (2005). Categorías de datos reconocidas en la Ley 19.628. *Revista Chilena De Derecho Informático*, (6).

Jijena Leiva, Renato (2009). *Informe Jurídico. Regulación jurídica de los sistemas de tratamiento de datos personales al interior de la Administración del Estado, y su armonización con la Ley 20.285 sobre transparencia y acceso a la información de los servicios públicos*. https://archives.cplt.cl/transparencia_activa/RESPUESTASAI/S313.pdf.

Jijena Leiva, Renato (2013). Tratamiento de datos personales en el Estado y acceso a la información pública. *Revista Chilena de Derecho y Tecnología 2*(2), 49-94.

Lynskey, Orla (2016). The Europeanisation of data protection law. *Cambridge Yearbook of European Legal Studies 19*, 1-35.

Mantelero, Alessandro (2015). Smart cities, movilidad inteligente y protección de los datos personales. *IDP. Revista de Internet, Derecho y Política*, N° 21, 37-49.

Matus, Jessica (16 de junio de 2021). Una respuesta sensata a la protección de datos. *Diario Financiero*. https://www.df.cl/noticias/opinion/columnistas/una-respuesta-sensata-a-la-proteccion-de-datos/2021-06-16/183834.html.

Momberg Uribe, Rodrigo (2017a). Acciones colectivas y Ley N° 19.628 sobre protección de la vida privada y de datos de carácter personal. *Revista Chilena de Derecho Privado* (28), 357-363.

Momberg Uribe, Rodrigo (24 de julio de 2017b). La Corte Suprema y los datos personales. *El Mercurio Legal*. https://www.elmercurio.com/legal/movil/detalle.aspx?Id=905790&Path=/0D/D/.

Nacrur Gazali, Miguel Ángel y Ried Undurragfa, José Miguel (2020). Atribuciones de la Comisión para el Mercado Financiero. En Roberto Ríos (Coord.), *La Comisión para el Mercado Financiero* (pp. 63-102). Ediciones UC.

Pessó, Alex (17 de junio de 2021). El Sernac y la protección de datos. *Diario Financiero*. https://amp.df.cl/noticias/opinion/cartas/el-sernac-y-la-proteccion-de-datos/2021-06-17/182152.html.

SERNAC (4 de julio de 2012a). *Sernac oficia a Banco de Chile por error en envío de cartolas*. https://www.sernac.cl/portal/604/w3-article-2557.html.

SERNAC (13 de julio de 2012b). *Banco de Chile deberá pagar a los afectados por error en cartolas y los asegurará ante fraudes*. https://www.sernac.cl/portal/604/w3-article-2560.html.

Viollier, Pablo (2017). *El Estado de la Protección de Datos Personales en Chile*. Derechos Digitales.

Viollier, Pablo y Canales, María Paz (2018). La compatibilidad de la retención general de metadatos y el respeto a los derechos fundamentales: el caso del decreto espía. *Anuario de Derecho Público* 2018, 155-171.

Yuraszeck Krebs, Nicolás (2021). Sobre la proliferación de reguladores en materia de seguridad de la información. *Actualidad Jurídica*. https://actualidadjuridica.doe.cl/sobre-la-proliferacion-de-reguladores-en-materia-de-seguridad-de-la_informacion/

Zaror, Danielle (22 de junio de 2021). Datos personales y protección del consumidor (I). *Diario Financiero*. https://www.df.cl/noticias/opinion/cartas/datos-personales-y-proteccion-del-consumidor-i/2021-06-22/182342.html

Normativa citada

Ley N° 19.628 de 1999. Sobre protección de la vida privada. 28 de agosto de 1999.

Ley N° 19.496 de 1997. Establece normas sobre protección de los derechos de los consumidores. 7 de marzo de 1997.

Ley N° 20.575 de 2012. Establece el principio de finalidad en el tratamiento de datos personales. 17 de febrero de 2012.
Ley N° 20.285 de 2008. Sobre acceso a la información pública. 20 de agosto de 2008.
Ley N° 21.000 de 2016. Crea la Comisión para el Mercado Financiero. 23 de febrero de 2017. D.O. N° 41.692.
Ley N° 21.130 de 2019. Moderniza la legislación bancaria. 12 de enero de 2019. D.O. N° 42.252.
Ley N° 21.236 de 2020. Regula la portabilidad financiera. 9 de junio de 2020. D.O. N° 42.676.
Ley N° 20.584 de 2012. Regula los derechos y deberes que tienen las personas en relación con acciones vinculadas a su atención en salud. 24 de abril de 2012. D.O. N°
D.F.L. N° 3, de 1997, del Ministerio de Hacienda, que fija el texto refundido, sistematizado y concordado de la Ley General de Bancos. D.O. N° 35.944.
Decreto N° 1 de 2006 [con fuerza de ley]. Fija texto refundido, coordinado y sistematizado del decreto ley N° 2.763, de 1979 y de las leyes N° 18.933 y N° 18.469. 24 de abril de 2006. D.O. N°

Jurisprudencia citada

Servicio Nacional del Consumidor con Ticketmaster Chile S.A. (2016): Corte Suprema, 7 de julio de 2016 (Rol N° 1533-2015). Segunda Sala. [Recurso de casación]
Servicio Nacional del Consumidor con Créditos Organización y Finanzas S.A. (2016): Corte Suprema, 11 de octubre de 2016 (Rol N° 4903-2015). Segunda Sala. [Recurso de casación].
Servicio Nacional del Consumidor con Ticketek Co. SpA (2016): Corte Suprema, 6 de diciembre de 2016 (Rol N° 26932-2015). Segunda Sala. [Recurso de casación].
Contraloría General de la República. Dictamen N° 041188-17, de 24 de noviembre de 2017.
Control de constitucionalidad del proyecto de ley que modifica ley N° 19.496, sobre Protección de los Derechos de los Consumidores, correspondiente al boletín N° 9369-03. Ley N° 21.081 (2018): Tribunal Constitucional, 18 de enero de 2018 (Rol N° 4012-17). Pleno [Recurso de reconsideración].
Contraloría General de la República. Dictamen N° 011167-19, de 12 de agosto de 2019.
Contraloría General de la República. Dictamen N° 008113-20, de 20 de abril de 2020.
Contraloría General de la República. Dictamen N° 009545-20, de 01 de junio de 2020.
Contraloría General de la República. Dictamen N° 30041-20, de 25 de agosto de 2020.
Contraloría General de la República. Dictamen N° 37912-20, de 23 de septiembre de 2020.
Zuchel Matamala con Directora Zonal Centro Sur de Fonasa (2020): Corte Suprema, 5 de octubre de 2020 (Rol N° 21137-2020). Tercera Sala. [Recuso de apelación].
Vaccarezza con Fondo Nacional de Salud (2021): Corte Suprema, 13 de septiembre de 2021 (Rol N°38554-2021). Tercera Sala. [Recurso de apelación].
Reyes con Fondo Nacional de Salud (FONASA) (2021): Corte Suprema, 22 de octubre de 2021 (Rol N° 49703-2021). Tercera Sala. [Recurso de apelación]