



Revista de Derecho - Universidad
Católica del Norte

ISSN: 0717-5345

revistaderecho@ucn.cl

Universidad Católica del Norte
Chile

ÁLVAREZ VALENZUELA, DANIEL

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, vol. 23, núm. 1, junio, 2016, pp. 51-
79

Universidad Católica del Norte
Coquimbo, Chile

Disponible en: <http://www.redalyc.org/articulo.oa?id=371046600003>

- Cómo citar el artículo
- Número completo
- Más información del artículo
- Página de la revista en redalyc.org

redalyc.org

Sistema de Información Científica

Red de Revistas Científicas de América Latina, el Caribe, España y Portugal

Proyecto académico sin fines de lucro, desarrollado bajo la iniciativa de acceso abierto

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?*

DANIEL ÁLVAREZ VALENZUELA**

RESUMEN: El presente trabajo analiza la posibilidad de transformar al Consejo para la Transparencia en la agencia pública que vele, al mismo tiempo, por el acceso a la información pública y la protección de datos personales. Para ello, esbozaremos el alcance de la protección de datos personales, describiendo el estado de la discusión sobre la necesidad de contar con una autoridad de control, para luego, identificar las razones que justificarían transformar a ese Consejo, recogiendo las principales críticas.

PALABRAS CLAVE: Protección de datos personales - autoridad de control - acceso a la información pública - Consejo para la Transparencia - Derecho Informático - Privacidad.

ACCESS TO PUBLIC INFORMATION AND DATA PROTECTION. CAN THE COUNCIL FOR TRANSPARENCY BE THE SUPERVISORY AUTHORITY ON DATA PROTECTION?

ABSTRACT: This paper analyzes the possibility of transforming the Council for Transparency in the public agency to ensure at the same time, access to public information and protection of personal data. To do this, the scope of protection of personal data will be outlined by describing the state of the discussion about the need for a supervisory authority. The

* El presente trabajo fue realizado con la importante colaboración de la señorita Rayén Campusano Barra, ayudante de investigación del Centro de Estudios en Derecho Informático de la Universidad de Chile y fue comentando por el profesor Alberto Cerda Silva, a quienes agradezco sus contribuciones y comentarios.

Fecha de recepción: 26 de marzo de 2015.

Fecha de aceptación: 27 de agosto de 2015.

** Abogado. Licenciado en Ciencias Jurídicas y Sociales y Diplomado en Derecho Informático, ambos por la Universidad de Chile (CHILE). Profesor de Privacidad y Tecnología. Facultad de Derecho, Universidad de Chile (CHILE). Coordinador de Investigación del Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile y Fundador y Editor General de la Revista Chilena de Derecho y Tecnología. Fundador de ONG Derechos Digitales. Correo electrónico: dalvarez@uchile.cl.

reasons that justify the transformation of the Council will be identified afterwards by acquiring the main review.

KEYWORDS: Data protection - access to public information - Council for Transparency - Cyber Law - privacy.

Sumario: Introducción. 1) El derecho a la vida privada en Chile y la protección de datos personales. 1.1) El consenso que ya tenemos: Chile necesita una autoridad de control. (2) La transparencia de la actividad pública en Chile. (3) El conflicto evidente y su solución orgánica. 2) ¿Puede el Consejo para la Transparencia ser la autoridad administrativa de control en materia de protección de datos personales? (1) ¿Por qué es necesaria una autoridad de control en materia de protección de datos personales? (2) El CPLT como autoridad de control en materia de protección de datos personales. (3) Otorgarle al CPLT las atribuciones, funciones y facultades necesarias para constituirlo en el órgano de promoción y protección de la vida privada tanto para el sector público como privado. (4) Las críticas a la propuesta. Conclusiones.

INTRODUCCIÓN

Desde antes de la entrada en vigencia de la Ley N°19.628 sobre Protección de la Vida Privada¹ (en adelante, "LPVP"), se discute acerca de la necesidad de establecer una autoridad pública que se encargue de fiscalizar el cumplimiento efectivo de sus disposiciones.

Con los años, el escaso número de acciones de *habeas data* que se han interpuesto ante los tribunales ordinarios de justicia y la creciente importancia que la protección del derecho a la vida privada, en sus múltiples dimensiones, ha ido adquiriendo en la vida cotidiana de las personas, exige retomar esta discusión.

En paralelo, desde la puesta en marcha del Consejo para la Transparencia² (en adelante, "CPLT" o "el Consejo"), órgano que en el ejercicio de sus funciones debe resolver continuamente asuntos que ponen en tensión el principio de transparencia en la función pública con el derecho a la vida privada de las personas, se ha discutido acerca de la posibilidad de que dicho órgano asuma la función de autoridad de control en materia de protección de datos, tanto respecto del sector público como del privado, ampliando sus actuales atribuciones. El objeto del presente trabajo es analizar esta posibilidad.

¹ Publicada en el *Diario Oficial* con fecha 28 de agosto de 1999.

² Creado por Ley N°20.285, publicada en el *Diario Oficial* con fecha 20 de agosto de 2008.

1) EL DERECHO A LA VIDA PRIVADA EN CHILE Y LA PROTECCIÓN DE DATOS PERSONALES

El derecho a la vida privada en Chile está configurado en la garantía del numeral 4° del artículo 19 de la Constitución Política, que asegura a todas las personas "el respeto y protección a la vida privada" y, especificado, en el ámbito del hogar, de las comunicaciones y de los documentos privados, en la garantía de inviolabilidad establecida en el numeral 5° del mismo artículo.

Ambas disposiciones, junto a las normas pertinentes de los tratados internacionales sobre derechos humanos suscritos y ratificados por Chile y que se encuentren vigentes³, forman parte del denominado bloque constitucional⁴ de protección de la vida privada, que debe guiar las decisiones legislativas que buscan materializar y concretizar dicha protección.

En materia de protección de datos personales, la concreción legal del bloque constitucional está contenida en la ya mencionada Ley N° 19.628, que sin perjuicio de nominarse «sobre protección de la vida privada», más bien trata sobre la regulación legal del mercado de tratamiento de datos personales⁵.

Si bien la ley reconoce una serie de derechos a las personas naturales titulares de los datos, estos deben ser ejercidos ante tribunales civiles, en procedimiento de larga y costosa tramitación⁶, lo que constituye una barrera para el ciudadano común. A la fecha, luego de quince años de

³ Véase los artículos 12 de la Declaración Universal de Derechos Humanos; V, IX y X de la Declaración Americana de Derechos y Deberes del Hombre; 17 del Pacto Internacional de Derechos Civiles y Políticos; y, 11 del Pacto de San José de Costa Rica.

⁴ El concepto doctrinario de bloque constitucional de derechos fundamentales fue recientemente reconocido, por primera vez, en una sentencia del Tribunal Constitucional de Chile. Véanse los considerandos séptimo y octavo de TRIBUNAL CONSTITUCIONAL. 6 de mayo de 2014. Rol 2493-INA. "Requerimiento de inaplicabilidad por inconstitucionalidad presentado por Enrique Eichen Zambrano respecto del artículo 5°, numerales 1°, inciso primero, y 3° del Código de Justicia Militar". Disponible en <http://www.tribunalconstitucional.cl/wp/ver.php?id=2968> [fecha de visita 25 de marzo de 2015].

⁵ Según JIJENA "la Ley sobre Protección de Datos Personales, N° 19.628 del año 1999, fue redactada con la asesoría directa de grupos, gremios y empresas interesadas en asegurar el negocio que constituye el procesamiento de datos personales, lo que se sumó al desconocimiento de los parlamentarios que la impulsaron." JIJENA, Renato (2010). "Actualidad de la protección de datos personales en América latina. El caso de Chile". En VV.AA: *Memorias del XIV Congreso Iberoamericano de Derecho e Informática*. Monterrey, UNAM, pp. 413 – 431, p. 414.

⁶ Si bien la Ley 19.628 establece un procedimiento especial denominado *habeas data*, el cual debe tramitarse breve y sumariamente, la administración civil de justicia presenta retrasos considerables en toda su gestión, lo que ha dado origen al diseño de un nuevo procedimiento civil, el cual está actualmente en discusión en el Congreso Nacional (Boletín N° 8197-07).

vigencia de sus normas, no existe jurisprudencia civil relevante que haya sancionado el tratamiento indebido de datos personales⁷.

Ante la situación de desprotección de los derechos de los titulares de datos personales, algunos han debido recurrir a otras medidas judiciales, como la acción de protección por afectación de garantías constitucionales, con resultados inciertos y poco estandarizados, lo que tampoco otorga un adecuado nivel de protección de los derechos de las personas⁸.

Por otra parte, desde la aprobación de la ley en 1999, la preocupación por la protección de los datos personales en particular y por la protección de la vida privada de las personas en general, ha aumentado de manera importante, motivada quizás por el desarrollo de tecnologías que facilitan el procesamiento de grandes volúmenes de datos personales, a bajo costo.

Dicha preocupación se ha visto reflejada, por ejemplo, en el trabajo del Congreso Nacional, donde se han presentado más de setenta y dos iniciativas legislativas (entre mociones y mensajes)⁹ que buscan perfeccionar la protección de los datos personales o establecer nuevas reglas en algunos sectores, como se aprecia en el gráfico siguiente. Solo seis de estas iniciativas han sido aprobadas y, lamentablemente, constituyen reformas menores o demasiado específicas¹⁰.

⁷ Revisadas las bases de datos del Poder Judicial, fue posible encontrar apenas una treintena de sentencias dictadas por tribunales de primera instancia relativas al ejercicio de la acción de *habeas data* que contempla la LPVP, en el período comprendido entre el año 2000 y 2014. En cambio, en el mismo período, es posible encontrar más de cuatrocientas sentencias de la Corte Suprema recaídas en recursos de protección por vulneración del derecho a la vida privada, de las cuales aproximadamente un 25% corresponden a casos relativos a datos personales. Las estadísticas anteriores forman parte de un proyecto de investigación dirigido por el autor, cuyos resultados serán publicados durante el año 2016.

⁸ Para una visión general, aunque limitada hasta el año 2010, de la jurisprudencia de protección en materia de derecho a la vida privada, véase FIGUEROA, Rodolfo (2013). “El derecho a la privacidad en la jurisdicción de protección”. *Revista Chilena de Derecho*, vol. 40, N° 3, pp. 859-889.

⁹ Boletines números 2474-07, 2771-05, 3003-19, 3066-03, 3094-19, 3095-07, 3185-19, 3312-05, 3656-18, 3796-07, 4124-18, 4143-07, 4203-07, 4429-07, 4466-03, 4482-03, 4629-07, 4959-03, 4972-03, 5009-06, 5053-07, 5122-07, 5309-03, 5320-03, 5351-07, 5356-07, 5365-07, 5754-07, 5883-07, 5999-07, 6120-07, 6298-05, 6353-07, 6495-07, 6594-07, 6598-06, 6854-03, 6914-03, 6939-03, 6979-06, 6982-03, 6994-07, 7026-07, 7055-07, 7093-03, 7132-03, 7158-05, 7232-03, 7282-07, 7715-03, 7732-07, 7776-03, 7777-07, 7794-07, 7808-13, 7831-07, 7833-13, 7864-03, 7886-03, 8086-04, 8143-03, 8175-03, 8208-07, 8222-11, 8275-07, 8559-03, 8589-07, 9242-10, 9252-15, 9388-03, 9384-07 y 9308-07. El presente índice de boletines fue preparado por ALVARADO, Francisco (2013) “Internet y las fuentes de acceso público a datos personales”. Santiago, Tesis para optar al grado de Licenciado en Ciencias Jurídicas y Sociales, Universidad de Chile, y actualizada por la ayudante Rayén Campusano.

¹⁰ Se trata de los boletines números 2600-18 que dio origen a la Ley 20.152, la cual establece la comunicación en el Boletín Comercial de los incumplimientos graves de deudas alimenticias; 2735-05 que dio origen a la Ley 19.812 la que elimina información de carácter económico, financiero, bancario y comercial para favorecer la reinserción laboral de las personas

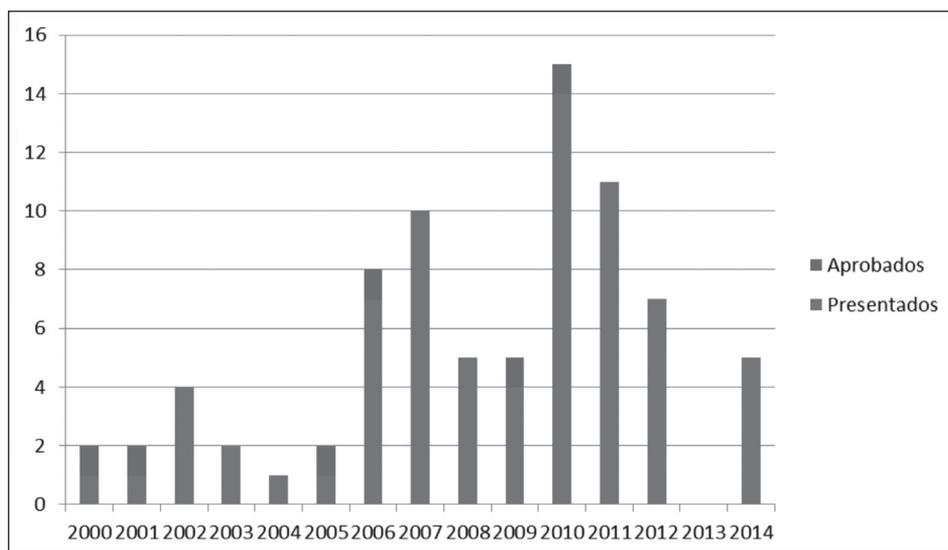


Ilustración 1. Proyectos de ley ingresados y aprobados en el Congreso Nacional sobre Datos Personales período 2000 - 2014. Elaborado por la ayudante Rayen Campusano.

Respecto a las reformas generales o estructurales al régimen de protección de datos personales, se han presentado y discutido solo dos iniciativas legislativas desde 1999 a la época.

La primera de ellas corresponde al proyecto de ley¹¹ ingresado en las postrimerías del primer gobierno de la presidenta Michelle Bachelet, el cual fue calificado como el más completo intento de elevar sustancialmente el estándar de protección de los datos personales en Chile¹². En lo que nos interesa, el proyecto proponía conceder facultades de autoridad de control en materia de protección de datos personales al Consejo para la Transparencia, pero no alcanzó a ser discutido en el Congreso Nacional.

desempleadas; 3773-06 que dio origen a la Ley 20.285 sobre acceso a la información pública; 4436-03 que dio origen a la Ley 20.463 que suspendiendo por un plazo determinado la comunicación de información comercial de las personas cesantes; 6800-03 que dio origen a la Ley 20.521 que prohíbe la realización de predicciones o evaluaciones de riesgo comercial basada en información que no sea objetiva; y, 7392-03 que dio origen a la Ley 20.575, que aclara la restricción de la comunicación de datos de carácter económico, financiero, bancario y comercial, también conocida como Ley Dicom.

¹¹ Boletín N°6120-07.

¹² SANZ, Francisco (2013). "Solicitud de acceso a la información y tutela de los datos personales de un tercero". *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, vol. XLI, pp. 457 - 502, p. 476.

La segunda iniciativa corresponde al proyecto de ley¹³ presentado durante la administración del presidente Sebastián Piñera, el cual proponía "entre otras reformas estructurales" entregarle al Servicio Nacional del Consumidor (en adelante, SERNAC), atribuciones específicas en materia de protección de datos personales respecto al tratamiento que realizaran privados. Este proyecto fue intensamente discutido en la Comisión de Economía de la Cámara de Diputados y fue objeto de importantes críticas en su propuesta de institucionalidad, al punto que las disposiciones específicas relativas al Sernac fueron rechazadas¹⁴.

En síntesis, el escenario regulatorio ha permitido que la información personal de los chilenos circule libre y legalmente por múltiples empresas dedicadas al tratamiento masivo de datos personales y sea intercambiada frecuentemente por compañías prestadoras de servicios comerciales, financieros, de salud, de telecomunicaciones, entre otras, vulnerando con ello el derecho a la vida privada y otros derechos amparados por la Constitución. Incluso, en los últimos años se ha denunciado el tráfico o filtración de bases de datos desde servicios públicos a entidades comerciales, prácticas que no han recibido sanción alguna.

(1.1.) EL CONSENSO QUE YA TENEMOS: CHILE NECESITA UNA AUTORIDAD DE CONTROL

Uno de los consensos que existe en materia de protección de datos es que Chile requiere de una autoridad de control que se haga cargo de promover, educar e informar a los ciudadanos sobre su derecho a la vida privada y a la protección de sus datos personales, fiscalizar el cumplimiento de la ley y sancionar las infracciones, entre otras funciones.

Antecedentes de esta necesidad podemos encontrar incluso antes de la dictación de la LPVP, tal como da cuenta la opinión del profesor Francisco CUMPLIDO, quien al analizar un anteproyecto de ley sobre protección de datos personales elaborado por el Ministerio de Justicia en el período 1990-1994, que contemplaba la creación de un "Servicio de protección de datos" y un "Registro Conservador o Registro de Datos", categóricamente sostuvo que «llegamos a la conclusión de que, para que pudiera ser efectiva y real la protección de los datos personales, era indispensable establecer un servicio del Estado que contribuyera a la protección de esos datos personales»¹⁵.

¹³ Boletín N° 8143-03.

¹⁴ Informe de la Comisión de Economía, Fomento y Desarrollo recaído en el proyecto de ley que introduce modificaciones en la ley 19.628, sobre protección de la vida privada. Boletín N° 8143-03. 10 de septiembre de 2014, pp. 89-90.

¹⁵ CUMPLIDO, Francisco (1997). "Análisis del anteproyecto de ley sobre protección de datos personales elaborado por el Ministerio de Justicia (1990-1994)". *Ius et Praxis* vol. 3, N° 1, pp. 201-207. p. 201.

Luego, durante el debate legislativo del proyecto de ley¹⁶ que dio origen a la LPVP, diversas voces opinaron respecto a esta necesidad. Así, por ejemplo, el profesor Renato JIJENA propuso «la creación de una institución especializada que se encargue de la tutela de la intimidad y permita, en ese sentido, la restauración de los derechos conculcados y la aplicación consiguiente de sanciones¹⁷».

Previamente, la Comisión de Constitución, Legislación y Justicia del Senado, en primer trámite constitucional, había prescindido de la necesidad de contar con una autoridad nacional de control de datos personales, teniendo presente las erradas conclusiones contenidas en un artículo de Stewart Dresner sobre el panorama de la legislación europea en materia de protección de datos personales, que anticipaba un modelo basado en la autorregulación, cuestión que el devenir del tiempo demostró no ser cierta¹⁸.

Tiempo después, la misma Comisión del Senado, esta vez en tercer trámite constitucional, sugirió al Ejecutivo el envío de una indicación que permitiera la creación de un órgano en la administración del Estado que, a lo menos, concentrara la función de registro de bases de datos personales públicas y privadas. De más está decir que la indicación nunca se presentó y, como efecto colateral, se eliminó la exigencia de registro de las bases de datos personales gestionadas por privados, cuestión que debiera ser rectificadas¹⁹.

Por su parte, en la doctrina nacional no es difícil encontrar diversas voces que claman por el establecimiento de algún tipo de autoridad de control en esta materia. En el foro público, cada vez con mayor fuerza, diversos académicos, profesionales, organizaciones de la sociedad civil y partes interesadas han llamado la atención acerca de la necesidad de contar con una agencia pública que proteja, promueva y fiscalice la aplicación de la ley.

Alberto CERDA, en su completísimo trabajo sobre autoridad de control, ha sostenido que «la obtención de un nivel de protección adecuado

¹⁶ Boletín N° 896-07, de 5 de enero de 1993, del H. Senador Eugenio Cantuarias.

¹⁷ Historia de la ley 19.628. Biblioteca del Congreso Nacional, p. 291 y ss.

¹⁸ El artículo de Dresner formaba parte de la obra colectiva “La protección de datos personales. Regulación nacional e internacional de la seguridad informática” coordinada por Santiago Ripol, que aparece citada en el informe de la Comisión. Historia de la ley 19.628. Biblioteca del Congreso Nacional, p. 114. En opinión de CERDA, el artículo de Dresner “resultó ser erróneo en sus supuestos y, en consecuencia, desacertado en sus conclusiones. (...) Desatinado, porque el desarrollo de la informática y las telecomunicaciones, lejos de desalentar el establecimiento de autoridades de control, lo ha alentado, si bien renunciando a la pretensión de realizar un control tan férreo como el previsto inicialmente en las primeras leyes de datos”. CERDA, Alberto (2003). “La autoridad de control en la legislación sobre protección frente al tratamiento de datos personales”. Santiago, Tesis para optar al grado de magíster en Derecho Público, Universidad de Chile, pp. 168-169.

¹⁹ Historia de la ley 19.628. Biblioteca del Congreso Nacional, p. 291 y ss.

para los derechos fundamentales de las personas concernidas por el tratamiento de datos supone, imprescindiblemente, incorporar en nuestra normativa una autoridad de control especialmente abocada a velar por el cumplimiento de la misma²⁰».

Pedro ANGUITA, por su parte, ha sostenido reiteradamente que «la inexistencia de una autoridad de control que posea facultades investigativas y sancionatorias debilita fuertemente un sistema de protección de datos dejando a las normas como las establecidas por el legislador chileno en un conjunto de buenas intenciones de carácter programático, pero inaplicables en la práctica²¹».

En similar sentido, Raúl ARRIETA afirma que «El hecho de no contar con una autoridad independiente que se encuentre permanentemente velando por el cumplimiento de la ley tanto por parte de los organismos públicos como privados, que tenga la posibilidad de aplicar sanciones por el incumplimiento y que tenga un fuerte rol de promoción de la protección de datos personales, es un vacío que quizás formalmente aparece como la mayor dificultad de Chile para cumplir el estándar internacional exigido²²».

El diagnóstico también es compartido por Gladys CAMACHO, quien sostiene que «una de las mayores debilidades del régimen de protección de datos radica en carecer de instrumentos jurídicos (recursos o acciones) de defensa ágiles y expeditos, sanciones claras a los infractores, así como de una autoridad especializada que se aboque a garantizar su buen funcionamiento y que cautele oportunamente los abusos en el tratamiento de datos y los pueda sancionar oportunamente²³».

Desde la sociedad civil, el grupo RES PÚBLICA, en su documento «95 propuestas para un Chile mejor» recoge también esta preocupación, proponiendo una serie de modificaciones a la legislación nacional sobre protección de datos personales, entre las cuales mencionan expresamente la «creación de una agencia autónoma e independiente que fiscalice, promueva y garantice la aplicación de la ley en lo que se refiera a datos personales. Bajo su supervisión estarían los organismos privados y públicos que manejen bases de datos con información personal, y mantendría un registro de las bases existentes con la identificación de sus responsables». Incluso, van más allá y sugieren que el «Consejo para la Transparencia

²⁰ CERDA (2003) 237.

²¹ ANGUITA, Pedro (2007). *La protección de datos personales y el derecho a la vida privada*. Santiago: Editorial Jurídica de Chile, p. 554

²² ARRIETA, Raúl (2009). "Chile y la protección de datos personales: Compromisos internacionales" En VV.AA, *Chile y la protección de datos personales: ¿están en crisis nuestros derechos fundamentales?* Santiago: Ediciones Universidad Diego Portales, p. 21.

²³ CAMACHO, Gladys (2014). "La protección de datos como frontera del derecho de acceso a la información". *Revista de Gestión Pública*, vol. III, N° 1, pp. 73 - 93, p. 81.

adopte estas labores, ampliando su mandato, y sin la necesidad de crear una institución²⁴».

En similar sentido se ha pronunciado la FUNDACIÓN PRO ACCESO, que a través de su presidente, Federico Allendes, han sostenido que «Chile necesita una institucionalidad de protección de datos²⁵».

Este amplio consenso, también se manifestó durante la discusión legislativa del último proyecto de ley²⁶ que proponía entregarle al Servicio Nacional del Consumidor, como ya dijimos, algunas atribuciones que la convertirían en una especie de autoridad de control respecto del tratamiento de datos personales que realizaran los privados, encomendando dicha función al CPLT, cuando el tratamiento se verificara por organismos públicos.

Durante la discusión en la Comisión de Economía de la Cámara de Diputados, el representante del Comité Retail Financiero, Claudio ORTIZ, expresó que eran «partidarios de implementar el modelo de los países desarrollados mediante la creación de un órgano especializado –Autoridad de Protección de Datos o equivalente–, autónomo, con un ámbito de gestión tanto en el sector público como privado», criticando la opción presentada por el Ejecutivo de la época, argumentando que estaba «lejos de garantizar un mejor resguardo de los datos personales, creando disputas de autoridad y alejándose de las recomendaciones y exigencias dadas por la Unión Europea^{27 28}».

El profesor Renato JIJENA criticó el proyecto de ley, en este aspecto, afirmando que pretendía «subsana la inexistencia de un órgano fiscalizador o Autoridad de Control, asignando competencia al efecto al Sernac en el sector privado y al Consejo de Transparencia en el sector público, sin conferir las competencias y herramientas necesarias a una autoridad autónoma para velar por el adecuado cumplimiento de las normas sobre protección de datos²⁹».

Por su parte, Ricardo GEBAUER, Director Legal de Dicom-Equifax, la principal empresa dedicada al tratamiento de datos personales en Chile, sostuvo expresamente «que se necesita un organismo autónomo e independiente que tenga facultades regulatorias y, cuando proceda, sancionatorias. Ello se cumple creando un órgano especial en la línea de los DPA (*Data Protection Authority*) que existen en la legislación comparada³⁰».

²⁴ RES PÚBLICA. Propuesta 33: Cautelar la efectiva protección de los datos personales.

²⁵ <http://m.terra.cl/noticia?n=1688287&>

²⁶ Boletín N°8143-03

²⁷ Informe de la Comisión de Economía, Fomento y Desarrollo, pp. 26-27.

²⁸ En similar sentido se pronunciaron los profesores Ernesto Evans y Patricio Zapata. Informe de la Comisión de Economía, Fomento y Desarrollo, p. 32.

²⁹ Informe de la Comisión de Economía, Fomento y Desarrollo, p. 31.

³⁰ Informe de la Comisión de Economía, Fomento y Desarrollo, p. 33.

Desde la sociedad civil, ONG DERECHOS DIGITALES alertó precisamente acerca de una de las principales debilidades del proyecto, la «falta de autoridades públicas con atribuciones sustantivas en materia de control de datos³¹».

Como se puede apreciar, constituye hoy una opinión generalizada y mayoritaria, la necesidad de contar con una autoridad de control en materia de protección de datos personales en Chile. El disenso se produce al momento de determinar qué órgano debiera ejercer dicha función. Las alternativas para el establecimiento de una autoridad de control en materia de protección de datos personales son varias. La primera, es la creación de una agencia autónoma constitucional, similar al CPLT, exclusivamente dedicada a la protección de datos personales; la segunda, es otorgarle al CPLT esa atribución; la tercera, encomendarle esa función a otros órganos del Estado, como el SERNAC, alguna superintendencia o, incluso, dispersar sus competencias entre distintos órganos públicos. Sobre este punto volveremos más adelante.

(1.2.) LA TRANSPARENCIA DE LA ACTIVIDAD PÚBLICA EN CHILE

En virtud de los principios de transparencia en la administración pública y publicidad de los actos de gobierno, son públicos los actos y resoluciones de los órganos del Estado, así como sus fundamentos y los procedimientos que utilicen, la información elaborada con presupuesto público y toda otra información que obre en poder de la Administración, cualquiera sea su formato, soporte, fecha de creación, origen, clasificación o procesamiento³², salvo que concurran algunas de las causales de reserva establecidas por ley³³.

En este sentido, la regla general que prima en la Administración del Estado es la publicidad de sus actos, por lo que la reserva de los mismos será siempre una cuestión excepcional y regulada por ley.

Desde 1999, Chile cuenta con una vasta legislación que regula mecanismos que incentivan la transparencia en la Administración Pública. Con la entrada en vigencia de la Ley N° 19.653 sobre Probidad Administrativa, se introdujeron importantes modificaciones a la Ley N° 18.575 sobre Bases Generales de la Administración del Estado, y se establece como pilar fundamental en la función administrativa del Estado, el principio de Probidad Administrativa de los actos de gobierno, regulando además un procedimiento para solicitar información, fijando causales de denegación de entrega de documentos, y por último, un mecanismo ju-

³¹ Informe ONG Derechos Digitales, p. 2.

³² Artículo 5° de la Ley 20.285

³³ Artículo 21 de la Ley 20.285.

dicial de amparo a favor del requirente en caso de que su petición no sea satisfecha.

Posteriormente, la reforma constitucional del año 2005 les confiere rango constitucional a los principios de transparencia en la administración pública y publicidad de los actos de gobierno los que se ven notoriamente fortalecidos.

Por último, con la promulgación de la Ley 20.285 sobre Acceso a la Información Pública, del año 2008, se generó el gran avance en materia de transparencia del sector público y acceso ciudadano, ya que dicho cuerpo legal fijó un nuevo marco normativo institucional que contempló el establecimiento de nuevos mecanismos para hacer efectiva la obtención de información pública, la regulación detallada de las causales de reserva y la creación de un órgano autónomo legal dotado de atribuciones fiscalizadoras y sancionadoras, el denominado Consejo para la Transparencia.

El Consejo, en sus cortos años de existencia, ha cumplido un rol gravitante no solo en crear una cultura sobre la transparencia del ejercicio de la función pública y en facilitar el acceso de la ciudadanía a la información pública, sino que también en definir los contornos de la tensión entre el acceso a dicha información y la protección de datos personales de los ciudadanos, a través de las decisiones que han adoptado en los amparos sometidos a su conocimiento, en un proceso que, por cierto, ha estado sujeto a múltiples críticas³⁴.

Asimismo, el Consejo, en ejercicio de la atribución establecida en el artículo 33 m) de la Ley 20.285, que le entrega la misión de velar por el debido cumplimiento de la LPVP por parte de los órganos de la Administración del Estado, publicó un conjunto de recomendaciones específicas que debieran ser observadas como guía o parámetro respecto del tratamiento de datos personales que se realizan los organismos públicos en el ejercicio de sus funciones³⁵.

³⁴ Un análisis detallado de la jurisprudencia emanada del CPLT en materia de protección de datos personales, es posible encontrar en CAMACHO (2014); MATUS, Jéssica (2013). "Derecho de acceso a la información pública y protección de datos personales". *Revista Chilena de Derecho y Tecnología*, vol. 2, N° 1, pp. 197 - 228. Con una mirada bastante crítica en JIJENA, Renato (2013). "Tratamiento de datos personales en el Estado y acceso a la información pública". *Revista Chilena de Derecho y Tecnología*, vol. 2, N° 2, pp. 49-94; y, GONZÁLEZ, Andrés y MELO Luis (2013). "Análisis crítico de la jurisprudencia del Consejo para la Transparencia a la luz de la normativa existente en materia de protección de datos personales". Santiago, Tesis para optar al grado de Licenciado en Ciencias Jurídicas y Sociales, Universidad de Chile, 439 pp. Un análisis más sistémico de la tensión entre ambas instituciones, es posible encontrar en SANZ (2013) 501, quien concluye que "la jurisprudencia del Consejo para la Transparencia, observa una clara tendencia a favor del acceso a la información pública por sobre la reserva o secreto de los datos personales. Sin embargo, en algunos casos la opinión de otras altas instancias del Poder Judicial (como es el caso del Tribunal Constitucional y las Cortes de Apelaciones) ha sido contraria a los argumentos propuestos por el órgano encargado de la transparencia".

³⁵ Publicada en el *Diario Oficial* del 14 de septiembre de 2011.

(1.3.) EL CONFLICTO EVIDENTE Y SU SOLUCIÓN ORGÁNICA

Es fácil imaginar los conflictos o tensiones que se pueden producir –y que de hecho se producen– entre acceso a la información pública y la protección de datos personales. Pareciera ser que están llamados a ser, en principio, antagónicos, y que la protección de uno implicará necesariamente la indefensión del otro.

Así, por ejemplo, un ciudadano en el ejercicio de su derecho de acceso a información pública puede terminar provocando la afectación del derecho de otro ciudadano cuyos datos personales forman parte de la información que se ha solicitado y que le ha sido entregada sin los debidos resguardos por parte del órgano de la administración.

Esta es una de las múltiples dimensiones posibles de la interacción entre transparencia y vida privada, existen muchísimas más. La evidencia indica que una cuarta parte de las decisiones de fondo dictadas por el CPLT en un trimestre determinado tenía relación con la protección de datos personales³⁶, información relevante al determinar la pertinencia de la pregunta planteada inicialmente y que abordaremos a continuación:

2) ¿PUEDE EL CONSEJO PARA LA TRANSPARENCIA SER LA AUTORIDAD ADMINISTRATIVA DE CONTROL EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES?

Para contestar esta pregunta responderemos previamente las siguientes interrogantes.

(2.1.) ¿POR QUÉ ES NECESARIA UNA AUTORIDAD DE CONTROL EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES?

Como ya se anticipó, existe un alto grado de consenso respecto a la necesidad de contar en Chile con una autoridad de control en materia de protección de datos personales. Sin perjuicio de ello, analizaremos algunas de sus razones.

Una primera lectura del artículo 1 de la LPVP nos indica que el tratamiento de datos personales solo puede hacerse en virtud de autorización legal o con consentimiento expreso del titular de los datos. Sin embargo, el contexto de esta normativa establece otra cosa: solamente se ha regulado el tratamiento de datos y no un derecho efectivo de los titulares a tener control sobre los mismos. Esto es así, entre otras razones, por la

³⁶ RAJEVIC, Enrique (2011). “Protección de datos y transparencia en la administración pública chilena: inevitable y deseable ponderación”. En VV.AA, *Reflexiones sobre el uso y abuso de los datos personales en Chile*. Santiago, Expansiva - Ediciones Universidad Diego Portales, p. 150.

inexistencia de un ente fiscalizador, de un procedimiento administrativo efectivo de reclamo y la falta de sanciones eficaces y disuasivas. Lo único que existe a este respecto es una acción judicial especial que se interpone ante los tribunales ordinarios, la acción de *habeas data* de escasa aplicación práctica³⁷.

La LPVP estableció una serie de principios aplicables al tratamiento de datos personales entre los cuales destacan el principio de licitud según el cual el tratamiento de datos solamente cabe si existe autorización legal o de parte del titular; el principio de información al titular respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público; el principio de veracidad de los datos, que exige corregir los que sean erróneos, inexactos, equívocos o incompletos; y, el principio de finalidad conforme al cual debe respetarse la finalidad informada al momento de recoger los datos, de manera que exista una relación directa entre aquella y el dato recabado.

Asimismo, la LPVP establece una serie de derechos a los titulares, como por ejemplo, el derecho que tiene toda 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 transmitidos³⁸; el derecho a que se modifiquen los datos personales que sean erróneos, inexactos, incompletos³⁹, etc. Sin embargo, estos derechos en la práctica no son respetados ya que, como hemos anticipado, la herramienta que contempla la LPVP en favor del titular de los datos personales se ejerce ante los tribunales ordinarios de primera instancia, que ha demostrado no cautelar efectivamente estos derechos.

Es una opinión compartida por buena parte de nuestra doctrina nacional, como ya vimos, que los derechos que consagra la LPVP no pasan de cumplir una mera función declarativa, a pesar de la enorme importancia que tienen la protección de datos personales para la vida cotidiana de las personas⁴⁰. Debemos recordar que los datos personales no solo constituyen un conjunto de información objeto de protección en beneficio de sus titulares (un «derecho», si así se prefiere) sino que también constituyen, en tanto conjunto de informaciones, un bien con valor económico que actualmente se transa en el mercado.

La importancia de la dimensión comercial del tratamiento de datos personales queda de manifiesto en el voto disidente de una sentencia del Tribunal Constitucional, en la que se expresa que el mundo moderno se

³⁷ Establecida en el artículo 16 de la LPVP.

³⁸ Establecida en el inciso primero del artículo 12 de la LPVP.

³⁹ Establecida en el inciso segundo del artículo 12 de la LPVP.

⁴⁰ CERDA (2003) 236; ANGUITA (2007) 554; JIJENA (2010) 414.

estructura en base al uso de la información. «El uso de ordenadores, el acceso a internet y a bases de datos permiten el procesamiento de gran cantidad de datos de todo tipo. Es cada vez más difícil sustraerse a esa realidad⁴¹». «Cabe resaltar que quienes hacen estas bases, en su gran mayoría, son privados. Desde el almacenero de la esquina hasta los grandes almacenes, bancos y casas comerciales, cada vez que una persona compra, salvo que sea en billetes, queda registrado lo que compra, cómo paga, las unidades que compra, etc. La vida comercial se construye de esa forma. Una interpretación extensiva del artículo 19 N° 4° de la Constitución, considerando solo la dimensión pasiva del derecho a la privacidad, pondría a nuestro comercio en una situación que le haría imposible crecer y desarrollarse⁴²».

Siendo esta doble dimensión correcta (derecho/bien) cabe preguntarse dos cosas. ¿Funciona el sistema de protección de derechos que establece la LPVP? ¿Funciona correctamente el mercado de tratamiento de datos personales? La respuesta a ambas preguntas no puede ser positiva.

Desde la dimensión «derecho» la respuesta es apabullante. Como reiteradamente hemos señalado, el nivel de desprotección del derecho de las personas a controlar el tratamiento que realizan terceros de sus datos personales es total. Se ha calificado a la ley y sus instrumentos como incapaz «de proporcionar una seguridad apropiada a la información personal, quedando muchos de sus artículos como letra muerta, entre otros factores, por la carencia de una institucionalidad a cargo del buen cumplimiento de la normativa⁴³».

Desde la dimensión «bien» basta apreciar el tráfico constante y permanente de información que existe entre operadores comerciales y los permanentes conflictos públicos que se generan por las prácticas de estos operadores, para intuir las razones de esta respuesta⁴⁴. En el mismo ámbito, esto es corroborado por las personas que "por ejemplo" tuvieron alguna morosidad que se tradujo en su inclusión en el Boletín Comercial,

⁴¹ Considerando trigésimo cuarto del voto disidente de los ministros señores Francisco Fernández y Carlos Carmona en sentencia TRIBUNAL CONSTITUCIONAL, 12 de julio de 2011. Rol N°1894-11. "Control de constitucionalidad del proyecto de ley que sanciona el acoso sexual de menores, la pornografía infantil y la posesión de material pornográfico infantil". Disponible en <http://www.tribunalconstitucional.cl/wp/ver.php?id=2011> [fecha de visita 25 de marzo de 2015].

⁴² TC. Rol N°1894-11. Dejo constancia que no comparto los fundamentos del voto disidente.

⁴³ Informe «Diseño de un modelo organizacional del Consejo para la Transparencia en su nueva función de protección de datos.» Centro de Sistemas Públicos. Departamento de Ingeniería Industrial, Facultad de Ciencias Física y Matemáticas, Universidad de Chile. 2010, p. 6.

⁴⁴ Basta recordar los casos de entrega irregular de datos personales entre farmacias e isapres, la filtración de bases de datos de usuarios desde el Registro Civil y la filtración de las bases de datos de FONASA a la multitienda La Polar, por mencionar los casos de mayor impacto público de los últimos años. Véase, a modo de ejemplo, <http://diario.latercera.com/2011/07/14/01/contenido/opinion/11-76348-9-filtracion-de-datos-de-fonasa.shtml>

posteriormente aclarada "mediante pago, prescripción, sentencia absolutoria, etcétera" y solicitan un crédito en un banco de la plaza; en ese momento se darán cuenta que esa morosidad sigue figurando en la base de datos bancaria respectiva, a pesar que el artículo 13 de la LPVP establece expresamente causales de caducidad del dato⁴⁵.

Sin embargo, al no existir una entidad estatal encargada de promover la protección efectiva de estos derechos, ¿quién se preocupa que los contratos que se firman masivamente en el *retail* no violenten la norma de orden público sobre caducidad?⁴⁶. ¿Quién promueve campañas de educación sobre la importancia de cuidar los datos personales en las redes sociales? ¿Quién investiga y sanciona las vulneraciones de datos personales? ¿Quién sanciona a las empresas que trafican datos personales de sus clientes?

Como se puede apreciar, el sistema de protección de datos personales que tenemos en Chile es reactivo, únicamente dirige los conflictos que el particular afectado promueve, en teoría, ante los tribunales ordinarios, y, en la práctica, por la vía de la acción constitucional de protección; no contamos con un sistema que promueva, proteja y promueva los derechos consagrados en la Constitución y en la LPVP, mediante la realización de acciones positivas tales como campañas de educación y difusión de estos derechos, por ejemplo.

Por ello, me sumo a la opinión mayoritaria que sostiene que es necesario dotar al país de un órgano de control que efectivamente vele por el cumplimiento de los derechos contemplados en la LPVP. Por los problemas anotados, es preciso contar con una agencia que se encargue no solamente de promocionar, proteger y promover los derechos establecidos en la LPVP sino que también velar porque estos se respeten mediante el ejercicio o la amenaza del ejercicio de la potestad sancionatoria.

Además, dicho órgano deberá velar porque los derechos consagrados en la LPVP se cumplan no solo en el ámbito de los servicios públicos sino que respecto de toda personas que realice tratamiento de datos personales.

⁴⁵ Véase la sentencia de la Corte Suprema recaída en el Recurso de Protección caratulado «Hidalgo Aguirre Rosa Myriam contra Banco BBVA», rol 1705-12, de 24 de septiembre de 2012, interpuesto por la recurrente al darse cuenta que figuraba en un registro informal y clandestino de deudores creado y mantenido por el recurrido, en el cual constaban obligaciones pagadas del año 2003. En el considerando duodécimo de la sentencia la Corte señala: «Que las conductas descritas conculcan el derecho constitucional de la recurrente previsto en el artículo 19 numeral 4º de la Constitución Política de la República, al afectar su honra, toda vez que es evidente que la inclusión de una deuda en un registro de morosidades desacreditada la fama de una persona cuando le imposibilita la obtención de un crédito por considerarla insolvente, cuando en realidad no lo es».

⁴⁶ Sin ir más lejos, en el año 2011 el Servicio Nacional del Consumidor denunció una serie de prácticas ilegales o abusivas de las compañías de telecomunicaciones en sus relaciones contractuales: obviamente dos de las diez prácticas identificadas dicen relación con el tratamiento indebido de datos personales de sus clientes. Véase <http://www.sernac.cl/sernac2011/noticias/detalle.php?id=2250>

En esta materia, el órgano de control deberá contar con funciones fiscalizadoras y ejercer la potestad sancionatoria directa contra particulares como a organismos públicos, ya que la imposición de multas u otro tipo de sanciones, incluso penales, corrigen el exceso de costo social que no asume la entidad privada o pública que infringe las normas de la LPVP.

(2.2.) EL CPLT COMO AUTORIDAD DE CONTROL EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

Antes de entrar en detalles, realizaremos una breve comparación del modelo de intervención en materia de transparencia y protección de datos en el caso de Chile y México, pues en este último país se ha optado por un modelo donde es la misma autoridad la que tienen por mandato legal garantizar, simultáneamente, el acceso a la información pública y la protección de datos personales de los ciudadanos.

En Chile, el CPLT es una corporación autónoma de derecho público, con personalidad jurídica y patrimonio propio, cuya dirección y administración superior corresponde a un cuerpo colegiado con facultades resolutivas⁴⁷, cuyos objetivos son: i) promover la transparencia de la función pública; ii) fiscalizar el cumplimiento de las normas de transparencia y publicidad de la información de los órganos de la administración del estado; y, iii) garantizar el derecho de acceso a la información⁴⁸.

En relación al tratamiento de datos personales el CPLT se ha pronunciado en cumplimiento de la función establecida en la letra m) del artículo 33 de la ley 20.285⁴⁹, mediante dos vías: 1) las partes han impetrado la protección de un dato personal y el CPLT ha debido referirse a ello en su decisión; o 2) el propio Consejo ha optado por aplicar directamente la legislación sobre protección de datos, sea porque esta aplicación inflúa en la decisión o se estimó que constituía una consideración adicional que debía tenerse en cuenta al momento de decidir el caso⁵⁰.

En México, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (IFAI) es un organismo descentralizado, no sectorizado, con personalidad jurídica y patrimonio propios⁵¹, cuya dirección y administración superior corresponden a un

⁴⁷ Artículos 31, 41, 36, 38 y 49 de la Ley 20.285.

⁴⁸ Artículo 32, de la Ley 20.285

⁴⁹ La letra m) del artículo 33, de la Ley 20.285 establece como atribuciones del Consejo: "Velar por el adecuado cumplimiento de la ley 19.628, de protección de datos de carácter personal, por parte de los órganos de la Administración del Estado".

⁵⁰ Informe sobre Jurisprudencia relevante del Consejo para la Transparencia en relación a la Protección de Datos Personales, Unidad Normativa, Dirección Jurídica del Consejo para la Transparencia, 1/2010-2011.

⁵¹ Artículo 33. Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

cuerpo colegiado (denominado Pleno) integrado por siete comisionados⁵², cuya misión es⁵³: i) garantizar el derecho de los ciudadanos a la información pública gubernamental y a la privacidad de sus datos personales; y, ii) promover en la sociedad y en el gobierno la cultura del acceso a la información, la rendición de cuentas y el derecho a la privacidad.

En materia de protección de datos, el IFAI es la autoridad garante del derecho de protección de datos personales y para el ejercicio de sus funciones cuenta con facultades informativas, normativas, de verificación, resolutorias y sancionadoras, conforme el siguiente detalle⁵⁴:

- Atribuciones informativas: proporciona apoyo técnico a quienes soliciten el cumplimiento de las obligaciones establecidas en la ley. Rinde cuenta al Congreso un informe anual de sus actividades. Desarrolla, fomenta y difunde análisis, estudios e investigaciones en materia de protección de datos personales en posesión de los particulares. Brinda capacitación a los sujetos obligados.
- Atribuciones normativas: interpreta la ley en el ámbito administrativo. Emite los criterios y recomendaciones. Divulga estándares y mejores prácticas internacionales en materia de seguridad de la información.
- Atribuciones de verificación: supervisa, vigila y verifica el cumplimiento de las disposiciones contenidas en la ley. Elabora estudios de impacto sobre la privacidad previos a la puesta en práctica de una nueva modalidad de tratamiento de datos personales o a la realización de modificaciones sustanciales en tratamientos ya existentes.
- Atribuciones resolutorias: Conoce y resuelve los procedimientos de protección de derechos y de verificación. Impone sanciones y las funciones en materia de cooperación como son acudir a foros internacionales y cooperar con otras autoridades de supervisión y organismos nacionales e internacionales, a efecto de coadyuvar en materia de protección de datos.
- Atribuciones sancionadoras: Impone sanciones pecuniarias. La ley prevé una serie de conductas consideradas como infracciones y sus sanciones, que van desde el apercibimiento hasta la imposición de multas máximas, bajo un sistema de modulación de la penalidad, de acuerdo con la gravedad de las conductas.

Para la imposición de sanciones, el IFAI debe tomar en cuenta factores como la naturaleza del dato; la notoria improcedencia de la negativa

⁵² IFAI ¿Qué es el pleno? <http://inicio.inai.org.mx/SitePages/queEsPleno.aspx>

⁵³ IFAI. Misión Visión y Objetivo. <http://inicio.inai.org.mx/SitePages/misionViosionObjetivos.aspx>

⁵⁴ IFAI. Cómo ejercer tu derecho a la protección de datos personales. <http://inicio.inai.org.mx/SitePages/Como-ejercer-tu-derecho-a-proteccion-de-datos.aspx?a=m3>

del responsable para realizar los actos solicitados por el titular; el carácter intencional o no de la acción u omisión constitutiva de la infracción; la capacidad económica del responsable y la reincidencia.

Contra las resoluciones del IFAI, las partes pueden promover el juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa. Lo que permite que los sujetos regulados cuenten con un medio de defensa idóneo y adecuado para la defensa de sus intereses y derechos en el orden administrativo.

La institucionalidad mexicana es de relativa novedad y no existen evaluaciones específicas sobre el desempeño de sus funciones, por lo que difícilmente se puede calificar su desempeño. Con todo, es un modelo de concentración en una sola institución de la administración del Estado de la misión de velar por la transparencia de la función pública y la protección de la vida privada de las personas, simultáneamente, que merece ser observado.

Como ya se dijo, en el caso de Chile, la injerencia del CPLT en materia de tratamiento de datos personales es indirecta, pues solo proporciona directrices en orden a limitar la intervención estatal –cuando es un órgano de la administración del Estado el que realiza el tratamiento de datos personales– o cuando debe resolver reclamaciones en solicitudes de acceso a información pública que contenga datos personales, conforme a la normativa legal, sin tomar un rol activo en la defensa y promoción del resguardo de los mismos⁵⁵.

Así, nuestro modelo institucional solo actúa en forma general mediante instrucciones y de forma particular a través de decisiones que resuelven amparos interpuestos por los afectados, siendo insuficiente su labor, dado que no logra tutelar –y no es su misión institucional hoy por hoy– en forma eficaz la garantía constitucional consagrada en el numeral 4° del artículo 19, materializada en la LPVP.

Pero esta situación es subsanable mediante una respuesta institucional, que analizaremos a continuación.

(2.3.) OTORGARLE AL CPLT LAS ATRIBUCIONES, FUNCIONES Y FACULTADES NECESARIAS PARA CONSTITUIRLA EN EL ÓRGANO DE PROMOCIÓN Y PROTECCIÓN DE LA VIDA PRIVADA TANTO PARA EL SECTOR PÚBLICO COMO PRIVADO

A modo preliminar es posible identificar varias razones para adoptar esta decisión. Revisemos las más importantes:

⁵⁵ Esta afirmación debemos matizarla respecto a las acciones de promoción y defensa que el CPLT ha realizado en materia de protección de datos personales cuando el responsable del tratamiento es un órgano de la administración del Estado, en ejercicio de las funciones encomendadas por el literal m) del artículo 33 de la Ley 20.285.

(2.3.1.) La mejor protección de ambos derechos

En materia de transparencia y acceso a la información pública, la labor del CPLT es encomiable. En pocos años, ha logrado aumentar el estándar de protección efectivo del derecho de la ciudadanía a acceder a información pública, consagrado indirectamente en la Constitución Política, además de promover, fortalecer y resguardar el ejercicio transparente de las funciones públicas, tanto a nivel central en la administración del Estado, como a nivel local, en gobiernos regionales, provinciales y municipales. Su proceso de instalación puede considerarse exitoso y no cabe más que esperar para el futuro la consolidación de los logros alcanzados.

En cambio, en materia de protección de datos personales, el escenario de desprotección es importante. Además de no ser considerados un país seguro para el tratamiento transfronterizo de datos personales, conforme los estándares establecidos por la Unión Europea⁵⁶, la realidad se encarga día a día de dar cuenta del lamentable estado de indefensión de estos derechos de las personas, como ya hemos visto.

De esta manera, creemos que si un órgano ha demostrado ser eficiente en el cumplimiento de su misión, como lo ha sido el CPLT dentro de su ámbito de funciones, también podría serlo si se amplían esas atribuciones, concediéndole competencias específicas en materia de protección de datos personales. Si además se le introducen las reformas orgánicas necesarias para evitar los riesgos que la concentración pudiere ocasionar y si se le dota de los recursos humanos y financieros necesarios, el resultado puede ser alentador.

Por ello, creo que es posible aventurar que de asumir el CPLT la función de autoridad de control en materia de protección de datos personales, mediante el ejercicio de las facultades de promoción y protección de los derechos establecidos en la LPVP y de sanción en casos de incumplimientos, el estándar de amparo del derecho a la protección de datos personales debiera experimentar algún tipo de alza.

Ante la ausencia total de control, el mero establecimiento de una agencia pública responsable, debiera impactar en la protección efectiva del derecho a tutelar⁵⁷. Si bien este sería un efecto que se podría producir

⁵⁶ Contenidos en 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.

⁵⁷ En similar sentido y teniendo presente la decisión política manifestada por el primer gobierno de Michelle Bachelet en el proyecto de ley contenido en el Boletín N°6120, el informe del Centro de Sistemas Públicos señala «La mayor factibilidad política planteada en el punto anterior se traduce en un acuerdo que acarrea una mejora en el corto-mediano plazo, velando por la protección de datos personales antes que en un escenario en el que se inicie una discusión sobre la institucionalidad asociada a la [protección de datos], lo cual podría retrasar aún más la aprobación del proyecto.» p. 112.

igual creando una autoridad de control independiente distinta del CPLT, el arbitraje interno de los conflictos o tensiones entre transparencia y protección de datos personales que deberá realizar el CPLT, es en mi opinión el factor clave que determinará el éxito o fracaso en el cumplimiento de su eventual nueva misión.

Cabe hacer presente que de tomarse los resguardos orgánicos, funcionales, de recursos humanos y de presupuesto necesarios, el ejercicio de las funciones actuales del CPLT no debieran verse mayormente afectadas, al contrario, podrían mejorar al incorporar en todo su quehacer institucional la dimensión de la protección de datos personales como parte esencial de su misión, cuestión que va en beneficio de ambas instituciones jurídicas⁵⁸.

(2.3.2.) El mejor arbitraje de conflictos entre transparencia y protección de datos personales

Teniendo presente las actuales competencias del CPLT y el desarrollo de una interesante jurisprudencia en la que ha intentado ponderar adecuadamente ambas instituciones —con importantes errores, por cierto—⁵⁹ le otorgan un grado de ventaja considerable en relación a cualquier otro órgano existente de la administración del Estado.

Hoy por hoy, el CPLT ya se preocupa, indirectamente, de la protección de la vida privada de las personas y sería necesario ampliar y mejorar esas competencias para transformarla en la autoridad de control en materia de protección de datos, incorporando esta función en su misión institucional y como un principio rector, en idéntica jerarquía, al principio de transparencia de la función pública⁶⁰.

Al interior del CPLT, se deberán realizar las reformas orgánicas necesarias para contar con dos instancias independientes entre sí pero dependientes del Consejo (en tanto órgano colegiado) responsable de ejecutar las funciones específicas que la ley les encomiende, entregando al Consejo la facultad para dirimir las controversias que se susciten entre estas instancias internas, cuyas máximas autoridades estarán siempre bajo dependencia jerárquica del CPLT.

⁵⁸ Un análisis detallado de las transformaciones que podría experimentar el CPLT en caso de asumir la función de autoridad de control en materia de protección de datos, es posible encontrar en la citado informe del Centro de Sistemas Públicos, pp. 26-71.

⁵⁹ Véase nota al pie número 63.

⁶⁰ Si bien el literal m) del artículo 33, de la Ley 20.285 le reconoce al Consejo la atribución de “Velar por el adecuado cumplimiento de la Ley 19.628, de protección de datos de carácter personal, por parte de los órganos de la Administración del Estado”, 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.

Respecto del Consejo mismo, se deberá ampliar su actual composición, estableciéndose una integración mixta e igualitaria de especialistas en materia de transparencia y protección de datos, respectivamente, además de especialistas en otras disciplinas que permitan contar con una mirada más amplia sobre los asuntos sometidos a conocimiento del cuerpo colegiado. La circunstancia de incorporar en el Consejo a personalidades destacadas del mundo de la protección de datos o de la privacidad es esencial para asegurar la permeabilidad de la actual composición y estructura orgánica del CPLT, que subsistiría probablemente a los cambios que se deban realizar⁶¹.

Con esta reformas estructurales, los casos en los cuales exista una tensión o conflicto entre la transparencia y el acceso a la información pública y el derecho a la protección de datos personales debieran ser resuelto satisfactoriamente en el seno del cuerpo colegiado integrado de la manera antes señalada, el cual sería el espacio de arbitraje o ponderación de los derechos de los administrados, que por ser una instancia administrativa no presenta grandes barreras de acceso para los ciudadanos, salvo en lo relativo a la descentralización territorial, cuestión que debiera ser subsanada⁶².

Este modelo permitiría resolver de manera expedita los casos frecuentes o rutinarios de conflictos entre derechos, lo que facilitaría, a su vez, generar lineamientos generales o específicos que la institucionalidad debiera recoger e implementar en su quehacer cotidiano.

Respecto a los casos complejos, esto es, aquellos donde el conflicto supone un enfrentamiento de posiciones o intereses derechamente contrapuestos, ya sean intereses económicos, políticos o sociales⁶³, la existencia

⁶¹ Un modelamiento de las diversas opciones para configurar el órgano decisorio de un futuro CPLT con facultades en materia de protección de datos, se presenta en el citado informe del Centro de Sistemas Públicos, pp. 46-58. En opinión de este autor, el modelo de consejo ampliado con delegación de funciones, consejeros suplentes e integrantes, con algunas modificaciones, podría resultar el más idóneo para asumir adecuadamente las nuevas atribuciones.

⁶² Actualmente, el CPLT solo tiene oficinas en la Región Metropolitana y para la interposición de reclamos en regiones, requieren de la colaboración de las Gobernaciones Provinciales.

⁶³ Dos de los casos más complejos que le correspondió decidir al actual CPLT, de manera errada, fueron los relativos a la privacidad de los correos electrónicos de funcionarios públicos, que dieron origen a dos sentencias del Tribunal Constitucional que junto con no acoger las alegaciones del CPLT, declararon inconstitucional algunas de las disposiciones claves de la ley N°20.285. Véase TRIBUNAL CONSTITUCIONAL. 11 de septiembre de 2011. Rol N° 2153-11. “Requerimiento de inaplicabilidad por inconstitucionalidad presentado por Rodrigo Ubilla Mackenney, Subsecretario del Interior, respecto del inciso segundo, del artículo 5° de la Ley N° 20.285, de 2008, sobre Acceso a la Información Pública”. Disponible en <http://www.tribunalconstitucional.cl/wp/ver.php?id=2537> [fecha de visita 25 de marzo de 2015]; y, Tribunal Constitucional. 31 de enero de 2013. Rol N° 2246. “Requerimiento de inaplicabilidad por inconstitucionalidad presentado por Claudio Alvarado Andrade, Subsecretario General de la Presidencia, en representación del Ministerio Secretaría General de la Presidencia, y Cristián Larroulet Vignau, Ministro Secretario General de la Presidencia, por sí, respecto del inciso segundo

"en todos los casos" de una instancia superior radicada en los tribunales de justicia, le concedería a las partes interesadas o, incluso, al propio Consejo, la posibilidad de arbitrar el conflicto ante un actor no involucrado en la discusión, con los riesgos y ventajas propias de ese sistema⁶⁴.

Esto es preferible frente a un sistema en el cual la autoridad de control en materia de protección de datos personales sea un organismo distinto al CPLT, por cuanto en ese caso habría que determinar de manera precisa sus características orgánicas (esto es, por ejemplo, si se trata o no de un órgano autónomo constitucional), el alcance de sus funciones, y un mecanismo externo de arbitraje de las diferencias que naturalmente se producirían entre ambas instituciones, lo que redundaría, probablemente, en un permanente conflicto de competencias que sería resuelto, conforme nuestro diseño constitucional, por un órgano con ningún nivel de experiencia en cualesquiera de ambas materias, con los riesgos propios que un sistema de esta naturaleza implica.

En conclusión, resulta una respuesta más consistente a la tensión entre ambas instituciones jurídicas, que sea un solo órgano el encargado de promover y proteger ambos derechos, tomando los resguardos institucionales ya descritos para evitar que uno de los principios, cualquiera de ellos, tenga preferencia por sobre el otro, debiendo resolverse siempre la tensión en cada caso concreto y estableciéndose mecanismos de arbitraje interno de las diferencias que se produzca en la forma de abordar esta misión institucional compartida. En cualquier caso, debieran establecerse mecanismos adicionales de control externo para evaluar el correcto desempeño de la institucionalidad.

(2.3.3.) Mayor eficiencia en la administración de los recursos fiscales

Como se puede imaginar, la creación de una nueva institución pública que se aboque únicamente a la protección de datos personales necesariamente requerirá de una mayor cantidad de recursos fiscales que centralizar en el CPLT dicha función. Desde el gasto en infraestructura, costos operacionales y recursos humanos, hasta los gastos de instalación y comunicaciones, supondrán siempre una inversión financiera mayor en el caso de crearse una nueva institución pública.

del artículo 5° de la Ley N° 20.285, sobre Acceso a la Información Pública." Disponible en <http://www.tribunalconstitucional.cl/wp/ver.php?id=2684> [fecha de visita 25 de marzo de 2015].

⁶⁴ El dejar la resolución de este tipo de conflictos en los tribunales de justicia, trae aparejado el delegar el establecimiento de políticas públicas en organismos no habilitados para ello. Traslado las competencias propias de los órganos del Estado o del Legislador, según corresponda, a los vaivenes de los criterios de equidad y justicia para cada caso en particular, amén de la falta de capacidades técnicas y de oportunidad de su actuar.

Por ello, aunar en un solo órgano público ambas funciones, permitirá hacer una gestión eficiente, desde el punto de vista de los recursos fiscales involucrados, mediante la ampliación de las competencias de una agencia que ya existe, siendo menores los costos operacionales, de infraestructura y recursos humanos. Sobre este punto, el informe del Centro de Sistemas Públicos de la Universidad de Chile sostuvo «Al tratarse de una única institución la que vela por los derechos de acceso a información pública y protección de datos personales, existe un ahorro de recursos al tener funciones que, en caso de estar en instituciones separadas, debieran duplicarse. Típicamente los procesos más estratégicos y transversales pueden tener economías de ámbito al estar radicados en una misma institución, y por ende reducir el costo país de introducir la función de protección de datos⁶⁵».

Sin perjuicio de ello, será necesario aumentar el correspondiente presupuesto anual del CPLT con el objeto de financiar las nuevas funciones a desempeñar y realizar las reformas orgánicas que se requieran para adaptar la institucionalidad actual a los nuevos requerimientos. Asimismo, como se anticipó, se deberá resolver la falta de descentralización que sufre el CPLT y promover la instalación de consejos regionales que asuman y ejerzan las funciones que la ley les mandate.

En conclusión, el reconocimiento del CPLT como autoridad de control en materia de protección de datos personales en Chile, con los resguardos necesarios ya identificados, puede significar por una parte, una mejora en la protección del derecho a la vida privada sin desmejorar el derecho de acceso a la información pública, y, por la otra, una mejor solución de los conflictos que enfrenten ambas instituciones jurídicas, mediante el arbitraje interno de las tensiones identificadas, además de establecer un modelo más eficiente en la administración de los recursos fiscales involucrados.

(2.4.) LAS CRÍTICAS A LA PROPUESTA

Por cierto que la propuesta de reunir en el CPLT las funciones de órgano garante de la transparencia y el acceso a la información pública y de autoridad de control de datos personales, no está exenta de críticas.

De partida, el informe del Centro de Sistemas Públicos de la Universidad de Chile, encargado por el propio CPLT en el contexto de la discusión del Boletín 6120-07, durante en el año 2010, identifica a los menos cuatro aspectos críticos: i) experiencia internacional; ii) las diferencias en

⁶⁵ Informe (2010) «Diseño de un modelo organizacional del Consejo para la Transparencia en su nueva función de protección de datos.» p. 111.

los "negocios": iii) capacidad del CPLT para fallar contra sí mismo; y, iv) concentración del arbitraje de conflictos. Revisemos cada una de ellas:

i) Respecto a la experiencia internacional, la observación del Centro de Sistemas Públicos no es conclusiva. Por una parte identifica a los países "principalmente europeos" que tienen agencias exclusivas en materia de protección de datos pero, a continuación, identifica a aquellos países que han optado por el modelo mixto aquí propuesto (Alemania, México, Reino Unido, Uruguay y Eslovenia)⁶⁶.

Sobre este punto, cabe señalar que la normativa comunitaria europea establece un mandato a los Estados miembros de establecer alguna autoridad de control en materia de protección de datos no existiendo dicho mandato en materia de transparencia y acceso a la información pública. De hecho, la principal autoridad de control de datos que frecuentemente se cita como modelo de éxito en la materia, la Agencia Española de Protección de Datos Personales (AEPD), conocida por su fuerza, capacidad y liderazgo, ha podido consolidar sus atribuciones⁶⁷, entre otras razones, precisamente porque en España no existe legislación sobre transparencia y acceso a la información pública. Resulta un ejercicio interesante imaginar cómo sería el desempeño de la agencia española de contar ese país con normas e institucionalidad sobre transparencia de la función pública. ¿Tendría la AEPD el mismo éxito si existiera una agencia pública de transparencia en España? Difícil de saber.

ii) Respecto a las diferencias de "negocios", el cual según el mencionado informe, se puede ver descrito en materia de principios, funciones, mercados y conflictos de intereses, es probablemente la crítica más importante.

Efectivamente, tal como sostiene JIJENA⁶⁸, la principal traba que existe para reunir en un solo órgano ambas funciones dice relación con los principios. Por una parte, los principios que inspiran los sistemas jurídicos que fomentan la transparencia y el acceso a la información pública tienen orígenes y focos que serían contradictorios con la idea de privacidad o autodeterminación informativa que está detrás de los regímenes de protección de datos personales.

Si bien ambos sistemas se basan en información (que puede o no ser información personal), unos propugnan la máxima apertura y transparen-

⁶⁶ Informe (2010) «Diseño de un modelo organizacional del Consejo para la Transparencia en su nueva función de protección de datos.» p. 110.

⁶⁷ De hecho, solo para ilustrar el poder que ha logrado la Agencia Española de Protección de Datos Personales, la más reciente sentencia del Tribunal Europeo de Justicia, recaído en el denominado Derecho al olvido en internet y que los enfrentó a una de las principales corporaciones internacionales, Google Inc., fue resuelto confirmando el criterio promovido por la Agencia. Véase Sentencia del Tribunal de Justicia. 13 de mayo de 2014. Asunto C-131/12.

⁶⁸ JIJENA (2013) 93.

cia posible, en tanto que los otros, abogan por su circulación restringida. El problema se presenta, entonces, como un binomio. La realidad nos dice otra cosa. Si bien es cierto el problema que se nos presenta, la armonización y ponderación de los derechos es un ejercicio que se debe realizar constantemente, tanto a nivel teórico como a nivel de protección efectiva de estos.

Es lo que no ocurrió, en mi opinión, en la criticable jurisprudencia administrativa emanada del CPLT en materia de inviolabilidad del correo electrónico de los funcionarios públicos, en la cual ha resuelto declarar como información pública⁶⁹ el contenido de esas conversaciones privadas, sin hacer una adecuada ponderación de las garantías de los numerales 4º y 5º del artículo 19 de la Constitución, cuestión que, en opinión de este autor y del voto de minoría de uno de los citados pronunciamientos, es inconstitucional⁷⁰. Esta fue precisamente la opinión del Tribunal Constitucional cuando conoció de estos casos en ejercicio de la acción de inaplicabilidad por inconstitucionalidad de un determinado precepto legal⁷¹. En ambos casos, el Tribunal declaró inaplicable por inconstitucionalidad el inciso segundo del artículo 5º de la Ley N°20.285 por afectación del numeral 5º del artículo 19 de la Carta Fundamental⁷².

Entonces, el obstáculo identificado, más que impedir la entrega de la función de autoridad de control en materia de protección de datos personales al CPLT, implica realizar y promover un debate acerca de la adecuada ponderación de los distintos derechos en juego en cada caso particular, lo que permitiría construir soluciones dotadas de legitimidad y racionalidad. Así, el desafío es cómo desde la cultura organizacional del CPLT y sus agentes, se promueve un ejercicio adecuado en la ponderación de derechos.

iii) Respecto a la capacidad del CPLT para fallar contra sí mismo, sin perjuicio de que se trata de una crítica que se puede formular a cualquier autoridad con facultades resolutorias, parte del control detentado sobre

⁶⁹ Decisiones C83-10, C126-11, C184-10 y C640-10.

⁷⁰ C640-10. El consejero señor Jaraquemada sostuvo que “revisar las comunicaciones electrónicas constituye una invasión de la intimidad personal y, por ende, su publicidad es constitucionalmente admisible únicamente en los casos y formas que prescribe la ley. Adicionalmente, como lo ha señalado reiteradamente el Tribunal Constitucional (...) la limitación de un derecho fundamental no puede ser tolerada si no está rodeada de suficiente determinación y especificidad como para garantizar una protección adecuada a la esencia del derecho y a su libre ejercicio, en este caso, el derecho a la privacidad y a la inviolabilidad de las comunicaciones privadas. 9º Que, en suma, la ley 20.285 no tiene la especificidad ni la determinación que le exige la Constitución para restringir el derecho que protege las comunicaciones vía correos electrónicos, pues no determina los casos ni las formas en que sería admisible la limitación de este derecho fundamental garantizado por el artículo 19 5 de la Constitución, en función de resguardar al máximo posible la intimidad y la vida privada”.

⁷¹ Establecido en el numeral 6º del artículo 93 de la Constitución Política.

⁷² Véase TC Rol N°2153-11 y TC Rol N° 2246-11.

los órganos del Estado está constituido por la aplicación a los principios inherentes a un estado de derecho, como son los principios de legalidad, control y responsabilidad administrativa, conformando así un sistema cautelar, al cual sin duda adscribe el CPLT. A ello se suma el control jurisdiccional sobre sus actos u omisiones⁷³.

Finalmente, cabe hacer presente que uno de los peligros más importantes del establecimiento de una agencia multisectorial como la descrita en la sección anterior, es su gran poder, lo que la hace susceptible a mayores focos de captura por parte de los particulares y del poder político. Frente a un conflicto de intereses las rentas derivadas de la captura se harán más atractivas cuando se trate de un mismo regulador⁷⁴. Con órganos independientes el centro de atención se diluye. De esta forma el mejor control ante las presiones públicas y privadas estaría dado por diversificar las competencias, pero las posibilidades de captura seguirán existiendo.

CONCLUSIONES

- Como hemos visto, desde antes de la entrada en vigencia de la LPVP se discute acerca de la necesidad de establecer una autoridad pública que se encargue de fiscalizar el cumplimiento efectivo de sus disposiciones.
- El escenario regulatorio ha provocado que la información personal en Chile circule libre y legalmente por múltiples empresas dedicadas al tratamiento masivo de datos personales y sea intercambiada frecuentemente por compañías prestadoras de servicios comerciales, financieros, de salud, de telecomunicaciones, entre otras, vulnerando con ello el derecho a la vida privada y otros derecho amparados por la Constitución.
- Uno de los consensos que existe en materia de protección de datos es que Chile requiere de una autoridad de control que se haga cargo de promover, educar e informar a los ciudadanos sobre su derecho a la vida privada y a la protección de sus datos personales, fiscalizar el cumplimiento de la ley y sancionar las infracciones, entre otras funciones. El disenso se produce al momento de determinar qué órgano debiera ejercer dicha función.
- Las alternativas para el establecimiento de una autoridad de control en materia de protección de datos personales son varias. La primera, es la creación de una agencia autónoma constitucional, similar al

⁷³ CERDA (2003) 197.

⁷⁴ GONZÁLEZ, Aldo (2006). “Estudio sobre la Revisión de la Institucionalidad Regulatoria de los Servicios sometidos a Fijación Tarifaria”. Santiago, Departamento de Economía de la Universidad de Chile, p. 21.

CPLT, exclusivamente dedicada a la protección de datos personales; la segunda, es otorgarle al CPLT esa atribución; la tercera, encomendarle esa función a otros órganos del Estado, como el Sernac, alguna superintendencia o, incluso, dispersar sus competencias entre distintos órganos públicos.

- La injerencia del CPLT en materia de tratamiento de datos personales es indirecta, pues solo proporciona directrices en orden a limitar la intervención estatal –cuando es un órgano de la administración del Estado el que realiza el tratamiento de datos personales– o cuando debe resolver reclamaciones en solicitudes de acceso a información pública que contenga datos personales, conforme a la normativa legal, sin tomar un rol activo en la defensa y promoción del resguardo de los mismos.

Pero esta situación es subsanable mediante una respuesta institucional: Otorgarle al CPLT las atribuciones, funciones y facultades necesarias para constituirlo en el órgano de promoción y protección de la vida privada tanto para el sector público como privado. El reconocimiento del CPLT como autoridad de control en materia de protección de datos personales en Chile, con los resguardos necesarios ya identificados, puede significar por una parte, una mejora en la protección del derecho a la vida privada sin desmejorar el derecho de acceso a la información pública, y, por la otra, una mejor solución de los conflictos que enfrenten ambas instituciones jurídicas, mediante el arbitraje interno de las tensiones identificadas, además de establecer un modelo más eficiente en la administración de los recursos fiscales involucrados.

BIBLIOGRAFÍA

- ALVARADO, Francisco (2013). Internet y las fuentes de acceso público a datos personales. Santiago, Tesis para optar al grado de Licenciado en Ciencias Jurídicas y Sociales, Universidad de Chile.
- ANGUITA, Pedro (2007). *La protección de datos personales y el derecho a la vida privada*. Santiago: Editorial Jurídica de Chile.
- ARRIETA, Raúl (2009). "Chile y la protección de datos personales: Compromisos internacionales". En VV.AA, *Chile y la protección de datos personales: ¿están en crisis nuestros derechos fundamentales?*. Santiago, Ediciones Universidad Diego Portales, pp. 13-22.
- CAMACHO, Gladys (2014). "La protección de datos como frontera del derecho de acceso a la información". *Revista de Gestión Pública*, vol. III, N° 1, pp. 73-93.

- CERDA, Alberto (2003). "La autoridad de control en la legislación sobre protección frente al tratamiento de datos personales". Santiago, Tesis para optar al grado de magíster en Derecho Público, Universidad de Chile.
- CUMPLIDO, Francisco (1997). "Análisis del anteproyecto de ley sobre protección de datos personales elaborado por el Ministerio de Justicia (1990-1994)". *Ius et Praxis* vol. 3 N°1, pp. 201-207.
- FIGUEROA, Rodolfo (2013). "El derecho a la privacidad en la jurisdicción de protección". *Revista Chilena de Derecho*, vol. 40, N°3, pp. 859-889.
- GONZÁLEZ, Aldo (2006). "Estudio sobre la Revisión de la Institucionalidad Regulatoria de los Servicios sometidos a Fijación Tarifaria". Santiago, Departamento de Economía de la Universidad de Chile.
- GONZÁLEZ, Andrés y MELO, Luis (2013). "Análisis crítico de la jurisprudencia del Consejo para la Transparencia a la luz de la normativa existente en materia de protección de datos personales". Santiago, Tesis para optar al grado de Licenciado en Ciencias Jurídicas y Sociales, Universidad de Chile.
- JIJENA, Renato (2010). "Actualidad de la protección de datos personales en América latina. El caso de Chile". En VV.AA. *Memorias del XIV Congreso Iberoamericano de Derecho e Informática*. Monterrey, UNAM, pp. 413-431.
- JIJENA, Renato (2013). "Tratamiento de datos personales en el Estado y acceso a la información pública". *Revista Chilena de Derecho y Tecnología*, vol. 2, N°2, pp. 49-94.
- MATUS, Jéssica (2013). "Derecho de acceso a la información pública y protección de datos personales". *Revista Chilena de Derecho y Tecnología*, vol. 2, N°1, pp. 197-228.
- RAJEVIC, Enrique (2011). "Protección de datos y transparencia en la administración pública chilena: inevitable y deseable ponderación". En VV.AA, *Reflexiones sobre el uso y abuso de los datos personales en Chile*. Santiago, Expansiva - Ediciones Universidad Diego Portales, pp. 137-159.
- SANZ, Francisco (2013). "Solicitud de acceso a la información y tutela de los datos personales de un tercero". *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, vol. XLI, pp. 457-502.

DOCUMENTOS

- Informe (2010) «Diseño de un modelo organizacional del Consejo para la Transparencia en su nueva función de protección de datos.» Centro de Sistemas Públicos. Departamento de Ingeniería Industrial, Facultad de Ciencias Física y Matemáticas, Universidad de Chile.

- Informe de la Comisión de Economía, Fomento y Desarrollo de la Cámara de Diputados (2013) recaído en el proyecto de ley que introduce modificaciones en la ley 19.628, sobre protección de la vida privada. Boletín N°8143-03.
- ONG DERECHOS DIGITALES (2012). *Minuta Proyecto de ley que introduce modificaciones a la Ley n°19.628 sobre protección de la vida privada y protección de datos personales*. <https://www.derechosdigitales.org/3342/comentarios-de-ong-derechos-digitales-a-proyecto-de-ley-de-datos-personales/>
- Recomendaciones del Consejo para la Transparencia sobre protección de datos personales por parte de los órganos de la administración del estado*. http://www.consejotransparencia.cl/consejo/site/artic/20121213/asocfile/20121213160518/proteccion_de_datos_web.pdf
- RES PÚBLICA (2013). *95 propuestas para un Chile mejor*. <http://95propuestas.cl/>