POTESTADES SANCIONATORIAS EN EL PROYECTO DE REFORMA A LA LEY Nº 19.628 DE PROTECCIÓN DE DATOS PERSONALES. UNA CRÍTICA[*]

Punitive powers in the Draft Amendments to the Law 19.628 on Personal Data Protection. A criticism

Pouvoirs de sanction dans les projets d'amendement à la Loi 19.628 sur protection des données personnelles. Une critique

Pablo Becerra Poblete[**]

Resumen

El presente trabajo analiza las potestades sancionatorias de los organismos competentes en el Proyecto de Reforma a la Ley Nº 19.628 sobre Protección de Datos Personales. Para ello, se analiza el modelo español de ejercicio de potestades sancionatorias para protección de datos personales, análisis del cual surgen elementos para criticar y revisar la configuración institucional escogida en nuestro Proyecto de Reforma, el cual, se concluirá, resulta inadecuado para tutelar el derecho fundamental a la autodeterminación informativa.

Palabras clave: Datos personales – Potestades sancionatorias – Ley Nº 19.628 – Agencia de Protección

Abstract

This paper analyzes the sanctioning powers vested upon the competent authorities in the Amendment Project for Act Number 19.628 on personal data protection. For such purpose, the Spanish sanctioning model for data protection enforcement is analyzed, thus providing elements to criticize and review the institutional configuration chosen in our Amendment Project, which, as we will show, is inadequate for an effective protection of the fundamental right to informational self-determination.

Key words: Personal Data – Sanctioning powers – Act Number 19.628 – Protection Agency

Resumé

Cet article analyse les pouvoirs de sanction des autorités compétentes dans le projet de loi de réforme Nº 19628 sur la protection des données personnelles. Nous analysons le modèle espagnol des pouvoirs de sanction pour protection des données personnelles, qui donnent des éléments d'analyse pour critiquer et revoir le cadre institutionnel choisi dans notre projet

[*] El artículo fue aprobado para su publicación el 15 de abril de 2013.

[**] Abogado. Licenciado en Ciencias Jurídicas y Sociales de la Universidad de Chile. Candidato a Magíster del Magíster en Derecho mención Derecho Público por la Universidad de Chile. Ayudante de las cátedras de Derecho Procesal y Clínicas Jurídicas de la Facultad de Derecho de la Universidad de Chile. Correo electrónico: pbecerrap@gmail.com.

Agradezco los valiosos comentarios del profesor Alberto Cerda Silva a una versión preliminar de este documento. Desde luego, las opiniones y errores son sólo míos.

de réforme, qui, a nos avis, est insuffisante pour protéger le droit à l'autodétermination informationnelle.

MOTS CLÉS: Données personnelles – Pouvoirs de sanction – Loi Nº 19628 – Agences de Protection

INTRODUCCIÓN

Un estudio publicado el año 2007[1], patrocinado por el Open Society Institute, sugiere que la protección de la privacidad en el mundo está empeorando a lo largo de las diversas jurisdicciones revisadas, como reflejo de un aumento en las políticas y sistemas de vigilancia pública y privada, y un detrimento correlativo de las barreras de protección de la privacidad. En particular, el estudio da cuenta de un aumento en la tendencia de los gobiernos a registrar y tratar datos geográficos, financieros y comunicaciones de sus ciudadanos y residentes, en lo que cabe denominar una verdadera "apropiación" pública de ámbitos privados[2-3]; tendencia que va de la mano con el nacimiento de una lucrativa industria de los datos personales dominada por empresas de internet y telecomunicaciones, de cuyos servicios los ciudadanos hacemos uso masivo, incluso inadvertidamente.

El uso masificado de las nuevas tecnologías de la información ha supuesto un cambio radical en nuestras formas de relacionarnos con nuestro entorno, comunicarnos, hacer negocios y llevar a cabo distintos aspectos de nuestras vidas, con lo cual una adecuada protección de los datos personales, particularmente (pero no únicamente) en lo relativo a entornos digitales, no sólo es un tópico urgente en aras de perfilar a nuestro país como una plataforma competitiva de *offshoring*[4] o

[1] PRIVACY INTERNATIONAL (2007). *The 2007 International Privacy Ranking.* Disponible en: <https://www.privacyinternational.org/article/leading-surveillance-societies-eu-and-world-2007#overview> [Consulta: 30 septiembre 2011].

[2] Sobre la expansión de lo público hacia el ámbito privado, por la vía de la "apropiación" de lo privado y la difusión de información de carácter personal, véase un interesante artículo de TAPIA RODRÍGUEZ, Mauricio (2008). "Fronteras de la vida privada en Chile". *Revista Chilena de Derecho Privado*, Fundación Fernando Fueyo, Nº 11. Disponible en: <http://www.fundacionfueyo.cl/revista/11_Revista_Fundacion_Fueyo.pdf> [Consulta: 30 septiembre 2011].

[3] Una de las áreas donde quizás más fuertemente se está impactando sobre el derecho a la privacidad y la autodeterminación informativa es en materia de propiedad intelectual, donde por vía de tratados internacionales (especialmente el *Anti-Counterfeiting Trade Agreement* o ACTA) pretenden incorporar normas autorizando la intrusión en los datos personales de los ciudadanos en niveles desproporcionados y mediante mecanismos sin precedentes, so pretexto de proteger derechos de propiedad intelectual. Sobre ACTA, véase: CERDA SILVA, Alberto (2011). "Enforcing Intellectual Property Rights by Diminishing Privacy: How the Anti-Counterfeiting Trade Agreement Jeopardizes the Right to Privacy". En: *Washington, American University International Law Review*, Washington College of Law, Vol. 26, Nº 3, pp. 601-643.

[4] *Offshoring* o *outsourcing* internacional es la subcontratación de procesos de negocios de un país a otro, usualmente en busca de costos más bajos o mano de obra. Incluye procesos como producción, manufactura, servicios e incluso innovación o investigación y desarrollo. Un típico ejemplo consiste en el establecimiento de un servicio de *call center* o centro de llamados para una empresa ubicada en otro país, de modo tal que la empresa se beneficie de los menores costos de operación del servicio en el país extranjero.

servicios globales con estándares internacionales de seguridad, y una plataforma competitiva de negocios y servicios, sino, ante todo, porque una adecuada protección de los datos personales incide directamente sobre el derecho fundamental a la autodeterminación informativa[5], e indirectamente, sobre otros derechos[6].

En este ámbito, y teniendo presente la variación de resultados del estudio para distintos países en el grupo pertinente, la Unión Europea se mantiene como "líder" en lo referente a protección de datos personales y la privacidad de sus ciudadanos. Las causas de ello son múltiples y complejas, pero en general dicen relación con la existencia de legislación robusta y coherente en materia de protección de datos personales, unida a un eficaz *enforcement* o régimen de cumplimiento de la legislación aplicable. Los resultados del estudio citado sugieren que incluso una legislación antigua y escueta arroja buenos resultados en cuanto a protección se refiere, si su régimen de cumplimiento es apropiado y efectivo.

En el presente trabajo, quisiera enfocarme en el segundo de los aspectos mencionados, es decir, cumplimiento. Más específicamente, quisiera analizar un particular componente del mismo, de cara al debate nacional sobre modificación de nuestra legislación de protección de datos: las potestades sancionatorias de los órganos competentes en materia de protección de datos personales. De este modo, mi objetivo consiste en efectuar una revisión de las potestades sancionatorias de la Agencia Española de Protección de Datos[7], con el objeto de proporcionar elemen-

[5] En España, la protección de los datos personales se ha desarrollado como integrante de un derecho fundamental autónomo, distinto a la privacidad o intimidad –el derecho a la autodeterminación informativa– principalmente a partir del artículo 18.4 de la Constitución Española (1978), el Convenio 108 de 1981 adoptado por la Comunidad Europea, y luego la Ley Orgánica 5/1992, 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal, hoy derogada y reemplazada por la Ley Orgánica 15/1999, 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD). Acerca del desarrollo jurisprudencial del derecho a la autodeterminación informática en España, véase en general: Lucas Murillo de la Cueva, Pablo (1999). "La Construcción del Derecho a la Autodeterminación Informativa". *Revista de Estudios Políticos*, España, Nº 104, abril-junio. Véase también: Cerda Silva, Alberto (2003). "Autodeterminación Informativa y Leyes sobre Protección de Datos". *Revista Chilena de Derecho Informático*, Santiago, Nº 3, pp. 63-65 y 69-70. Como hito jurisprudencial relevante en el desarrollo del derecho a la autodeterminación informativa como derecho autónomo en España, véase especialmente la Sentencia del Tribunal Constitucional español 292/2000, 30 de noviembre, fundamentos 6º, 7º y 11º.
El estado de la cuestión en el marco de nuestra Constitución Política de la República consiste en reconocer expresamente una protección al derecho a la intimidad ("respeto y protección a la vida privada y a la honra de la persona y su familia", artículo 19 Nº 4 CPR), a partir del cual, no obstante, puede construirse una protección normativa constitucional para el derecho a la autodeterminación informativa, de incipiente desarrollo en el ámbito local.

[6] Piénsese, por ejemplo, en la posibilidad que entidades o personas con poder de decisión o injerencia sobre aspectos de nuestra vida laboral, civil, política, íntima y otras, tuvieran bajo su poder información relevante acerca de estos aspectos de nuestras vidas, y pudieran tomar decisiones con esta información sin nuestro consentimiento o siquiera conocimiento. Ello da una idea de cómo la protección y control sobre nuestros datos personales incide en una manera muy real sobre la adecuada protección y libre goce y ejercicio de otros derechos fundamentales, como la libertad de expresión, la igualdad ante la ley, etc.

[7] La elección de la Agencia Española para realizar la comparación se justificó no sólo por el idioma de su legislación (facilidad de acceso y análisis), el puntaje relativamente alto obtenido por España en el estudio

tos para el análisis de la configuración institucional de las potestades sancionatorias en materia de protección de datos plasmadas en el Proyecto de Ley de reforma a la Ley Nº 19.628 chilena, que estuvo en consulta pública entre agosto y septiembre de 2011 a través del sitio en línea del Ministerio de Economía, Fomento y Turismo (en adelante, el "Proyecto de Reforma").

Resulta de sumo interés revisar las potestades sancionatorias de los organismos competentes de protección de datos, pues mediante tales potestades se articula una de las principales herramientas disciplinadoras de los agentes públicos y privados que intervienen en actividades de recopilación y tratamiento de datos personales, y se propende a mejorar los niveles de cumplimiento de la regulación de protección de datos. Al pensar en la protección de datos personales, consecuentemente, resulta fundamental no perder de vista nunca la necesidad de que el sistema de protección que se articule contemple mecanismos sancionatorios y sanciones efectivas que permitan disuadir con éxito las violaciones a los derechos de las personas. Como reflexiona ARRIETA, "no basta con que los derechos sean incorporados en la legislación, sino que también se hace necesario configurar un sistema complejo de protección de las personas que, junto con establecer y plasmar principios, implante mecanismos que permitan tutelar la efectividad de su cumplimiento"[8]. Y es que hablamos de *garantías fundamentales* porque ellas están establecidas para exigir su observancia de manera irrestricta, y en forma tal que su verificación sea permanentemente controlable por mecanismos institucionales estatuidos con dicha función. Lo central, entonces, es la posibilidad de tutela efectiva mediante mecanismos que nos permitan comprobar que la Constitución es algo más que un desiderátum. Como pretendo poner de manifiesto en el presente trabajo, valiéndome para ello del contraste de nuestro Proyecto de Reforma con la legislación española relevante, Chile tiene un largo camino que recorrer todavía en materia de protección de datos personales.

1. La Agencia Española de Protección de Datos (AEPD)

1.1. Generalidades

El marco regulatorio de la protección de datos personales a nivel estatal en España se articula a partir de la Ley Orgánica 15/1999, de 13 de diciembre, de

DOCTRINA

de protección a la privacidad citado en la nota 1, sino porque la legislación española ha sido un referente importante tanto para nuestra legislación de protección de datos personales vigente, como para el Proyecto de Reforma. "Este proyecto de ley se basa fundamentalmente en la ley orgánica Nº 1, de 5 de mayo de 1982, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, de España […]". HISTORIA DE LA LEY Nº 19.628, Biblioteca del Congreso Nacional, Moción Parlamentaria, p. 6.

[8] ARRIETA, Raúl (2009). "Chile y la Protección de Datos Personales". En: *Chile y la Protección de Datos Personales: ¿Están en Crisis Nuestros Derechos Fundamentales?* Expansiva, Santiago: Ediciones Universidad Diego Portales, p. 17. Disponible en: <http://www.expansiva.cl/media/publicaciones/libros/pdf/7.pdf> [Consulta: 13 noviembre 2011].

Protección de Datos de Carácter Personal (en adelante, "LOPD"), la cual materializa el mandato constitucional en orden a que "*La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*"[9].

La LOPD creó una entidad pública, independiente de la Administración del Estado, con personalidad jurídica propia y plena capacidad pública y privada, encargada de velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos; ente que recibe la denominación de Agencia Española de Protección de Datos (en adelante, "AEPD")[10].

La AEPD es encabezada por su Director, quien además ejerce la representación de la misma, nombrado entre quienes componen el Consejo Consultivo de la AEPD mediante Real Decreto. Dura en sus funciones un período de cuatro años, y cesa en ellas solamente por las causales taxativas establecidas en la propia ley[11]. Esta configuración del cargo Público de Director en la LOPD permite optimizar los niveles de independencia con respecto a otros poderes del Estado, toda vez que la permanencia en el cargo no se encuentra supeditada a decisiones discrecionales de otros organismos o poderes estatales (como es el caso de los llamados "cargos de confianza"), ni su proceso decisorio puede verse formalmente impactado por decisiones de otros poderes o de terceros. El Director de la AEPD ejerce su cargo con plena independencia y objetividad[12].

Las principales funciones de la AEPD en relación con el resguardo de los datos personales se contemplan en el artículo 37 de la LOPD, las cuales pueden sintetizarse en funciones de fiscalización y control del tratamiento de datos (artículo 37.A); información pública acerca de los derechos de las personas bajo la LOPD (artículo 37 D y E); velar por la publicidad de la existencia de los ficheros de datos personales existentes (artículo 37.J); funciones consultivas y reguladoras, y en lo que atañe al presente trabajo, se le encomienda el ejercicio

[9] Artículo 18.4, de la Constitución Española de 1978.

[10] La AEPD es regulada en el Título VI de la LOPD. Se rige por lo dispuesto en la LOPD y en el Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la LOPD; y por el Real Decreto 428/1993, 26 de marzo, que aprobó el Estatuto de la AEPD, modificado posteriormente por el Real Decreto 156/1996, 2 de febrero y el Real Decreto 1665/2008, 17 de octubre.

[11] Artículo 36.3 LOPD. No obstante, no deja de merecer reparos la relativa generalidad de la redacción de esta cláusula de remoción, y la posibilidad de que el Gobierno inste por tal remoción, aunque existen resguardos procedimentales que ponen coto a la influencia del Gobierno en esta materia.

[12] Para una breve caracterización general de las potestades del Director de la AEPD, el Consejo Consultivo y el Registro General de Protección de Datos, teniendo presente su carácter general debido a avances legislativos posteriores a su publicación, véase: Piñar Mañas, José Luis (2003). "La Agencia Española de Protección de Datos: Estructura y Funcionamiento". *Revista Chilena de Derecho Informático*, Nº 3, pp. 35 y ss.

de las potestades sancionatorias de conformidad con el Título VII de la LOPD (artículo 37.G).

Cabe destacar que la AEPD cuenta con un órgano integrado a su organización, denominado Registro General de Protección de Datos, cuya finalidad es la creación, registro y control de nóminas en las cuales se lleva constancia de forma permanentemente actualizada y pública de los ficheros de datos personales de titularidad pública y privada, y la demás información que ordena el artículo 39.2 LOPD en relación con los mismos[13].

El ejercicio de potestades sancionadoras bajo la LOPD no es la única competencia de este tipo de cargo de la AEPD, en cuanto la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI)[14] y la Ley General de Telecomunicaciones (LGT)[15] confirieron a la AEPD nuevas potestades sancionadoras bajo un marco regulador especial que apunta al derecho, tanto de personas naturales como jurídicas[16], a no recibir comunicaciones electrónicas con fines publicitarios o

[13] Por contraste, el artículo 9º del Proyecto de Reforma establece una obligación para el responsable del registro o banco de datos de mantener permanentemente a disposición del público a través de un sitio web un vínculo a través del cual puedan conocerse las bases de datos que administra, y mediante el cual cada titular de datos pueda realizar una búsqueda y así saber si sus datos forman o no parte de dichos registros. Vale decir, mientras la LOPD opta por la centralización de las bases datos en una "ventanilla única" a través de la cual pueden conocerse las bases existentes y la incorporación de un titular de datos en una de las bases, el Proyecto de Reforma chileno opta por la "atomización" de la información, debiendo recurrirse a cada uno de los innumerables entes en espera de conocer si tal o cual persona o ente maneja datos personales del titular o no. Creemos que ello impacta negativamente en la posibilidad de controlar el manejo que terceros hagan de los datos personales, puesto que dicho sistema supone que el titular conozca de antemano que un ente determinado posee información para dirigirse a su sitio; o bien, supone que el titular "salga de pesca" en innumerables sitios web, a la espera de encontrar alguno que registre información suya.
El deber contenido en el artículo 10 del Proyecto de Reforma –informar a los titulares de los datos tratados, a lo menos una vez al año, acerca de la existencia del archivo, registro, base o banco de datos personales, su finalidad y los datos específicos que en ella se contienen– es insuficiente para contrarrestar la elevada carga que su artículo 9º pone sobre los titulares de los datos a este respecto, pues, por una parte, el deber que impone el artículo 10 debe cumplirse tan sólo una vez al año, no obstante todas las modificaciones que puedan ocurrir en el tiempo intermedio; y por otra parte, el privado no se encontrará en posición de exigir responsabilidades en casos en que desconozca que un ente hace tratamiento de sus datos, e incumple el deber del artículo 10, pues, precisamente, desconoce que dicho ente trata sus datos (e incurre en infracción al no informárselo a lo menos anualmente).

[14] Ley Nº 34/2002, 11 de julio. Un interesante artículo sobre la protección en España de datos personales en materia de comercio y publicidad fue publicado en la Revista de Derecho Informático de la Universidad de Chile. Véase: FERNANDO MAGARZO, María del Rosario (2005). "La Protección de Datos Personales en el ámbito de la Publicidad en la Legislación Española". *Revista de Derecho Informático*, Nº 7, pp. 97-109.

[15] Ley Nº 32/2003, 3 de noviembre.

[16] En el marco de la LOPD, los derechos que ésta confiere dicen relación con personas naturales o físicas (véase artículo 3 A y D de la LOPD), excluyendo en general de la protección de datos personales a las personas jurídicas. A diferencia de la realidad española, el Proyecto de Reforma chileno pretende introducir cambios a la Ley Nº 19.628 de modo tal de extender su protección de manera general tanto a las personas naturales como a las personas jurídicas (en lo que resulte compatible para éstas), con

promocionales; cuestión distinta a la protección de datos personales propiamente tal, sin perjuicio de la evidente relación[17] entre ambos derechos[18].

1.2. AEPD y Agencias Autonómicas de Protección de Datos

De conformidad con el artículo 41 LOPD, y a la luz de las particularidades políticas del Estado español[19], algunas de las funciones de la AEPD son ejercidas por autoridades de control autonómicas cuando ellas inciden sobre ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas y por la Administración Local de su ámbito territorial, salvo ciertas excepciones contenidas en el propio artículo 41 LOPD, en cuyo caso la AEPD retiene la competencia. Cada órgano autonómico tiene la consideración de autoridad de control, y se les debe garantizar plena independencia y objetividad en el ejercicio de su cometido.

Existen hasta el momento tres Agencias Autonómicas de Protección de Datos: la de la Comunidad de Madrid, la Agencia Catalana y la Agencia Vasca[20], las que en todo caso, cabe recordarlo, tienen competencia sobre ficheros creados por las respectivas comunidades autónomas, o por la Administración Local de su ámbito territorial. En lo que excede de sus específicos cometidos, la AEPD retiene la competencia.

---

excepción de los datos definidos como sensibles, que, por su naturaleza, se estima que no les resultan aplicables a las últimas.

[17] La creación de bases de datos con correos electrónicos para el envío masivo de publicidad supone el tratamiento de datos personales tales como la casilla de correo electrónico y otros datos asociados a la misma, actividad que cae dentro del ámbito de aplicación de la LOPD, al igual que el tratamiento de dichos datos para ofertas por venta directa, vía fax o llamadas telefónicas automatizadas.

[18] Entre nosotros, el artículo 4.C del Proyecto de Reforma, incluye el deber de informar en toda comunicación comercial y publicitaria que se dirija nominativamente al titular de datos, el origen de los datos, la identidad del responsable del tratamiento y los derechos que le asisten. Estas comunicaciones no podrán dirigirse a titulares de datos que se hayan incluido en un registro electrónico dispuesto por el Servicio Nacional del Consumidor en su sitio web. Sin embargo, como veremos, el procedimiento para perseguir responsabilidades bajo esta norma implicará acudir a tribunales civiles bajo la forma de un juicio sumario especial, si el infractor es un ente privado, lo que desincentiva fuertemente la persecución de responsabilidades por infracciones a la norma.

[19] El Título VIII de la Constitución Española establece una división política del Estado en Municipios, Provincias y Comunidades Autónomas. Estas últimas gozan de competencias para gestionar sus propios intereses con un amplio nivel de autonomía legislativa, presupuestaria, administrativa y ejecutiva, respecto de las competencias exclusivas que el Estado les garantiza a través de la Constitución y de cada uno de los Estatutos de Autonomía.

[20] Acerca del reparto competencial entre la AEPD y las autoridades autonómicas de protección de datos, véase: López Román, Eduardo (2009). "Un Análisis de la Estructura Institucional de Protección de Datos en España". *Revista para el Análisis del Derecho (InDret)*, Barcelona, Nº 2, mayo, pp. 13-20. Disponible en: <http://www.indret.com/pdf/641_es.pdf> [Consulta: 17 septiembre 2011]. La misma fuente contempla un interesante análisis econométrico comparativo de la incidencia de estas distintas agencias en el cumplimiento de la normativa de protección de datos.

No obstante esta (relativa) pluralidad de órganos con competencia sobre protección de datos en España, cabe destacar que todos ellos son órganos de control a efectos de la LOPD, cuya finalidad es la protección de datos personales (es decir, son el órgano de control de la regulación de la LOPD con dedicación exclusiva) y demás funciones conexas; y en todos los casos se configuran como entes independientes de la Administración y de otros poderes, solamente pudiendo removerse a sus autoridades, en general, por causales legales taxativamente establecidas.

Recordemos, además, que el Director es independiente del Consejo Consultivo en el proceso de toma de decisiones, con lo cual se le dota de independencia funcional interna. El Consejo debe ser oído por el Director de la AEPD en las materias en que la propia ley así exige, pero sus opiniones no son vinculantes para el Director.

Lo que venimos comentando da cuenta de que España contempla un ente autónomo e independiente de control y protección de datos en su legislación, cuya finalidad exclusiva es, precisamente, su control y protección de conformidad con las normas de la LOPD. La manera de lograr dicha independencia radica de forma muy central en los mecanismos de nombramiento, los mecanismos de selección, las reglas de remoción y las reglas sobre responsabilidad, cuestiones sobre las que no podremos abundar aquí. La cualidad de independencia de la autoridad de control es consustancial a la institución de la autoridad de control, y un común denominador a las autoridades de control de protección de datos en Europa[21]. Como veremos, esta configuración institucional contrasta fuertemente con la realidad chilena.

1.3. Procedimiento sancionador

De conformidad con lo dispuesto en el artículo 48 de la LOPD, el procedimiento sancionador para la aplicación de la sanciones a que se refiere el Título VII de la LOPD se establece por vía reglamentaria, y en todo caso no debe durar más de seis meses. En virtud de dicha habilitación legal, el Reglamento de Desarrollo de la LOPD (en adelante, "RLOPD")[22], regula en su Título IX los procedimientos tramitados por la AEPD, entre los cuales se encuentran los procedimientos de tutela de los derechos de acceso, rectificación, cancelación y oposición (los cuales se inician a instancias del afectado, por medio de una presentación que cumpla con los requisitos establecidos en el artículo 117 del RLOPD); y en lo que respecta al objeto del presente trabajo, el procedimiento para el ejercicio de la potestad sancionadora. Este último procedimiento, de conformidad con lo dispuesto en el artículo 120 del RLOPD, es de general aplicación para el ejercicio de las po-

[21] Cfr. CERDA SILVA, Alberto (2005). *La Autoridad de Control sobre Protección de Datos Personales.* Universidad de Chile, Anales de la Facultad de Derecho, Santiago, Nº 2, pp. 42-47.

[22] Aprobado por el Real Decreto 1720/2007, 21 de diciembre.

testades sancionadoras bajo la LOPD, la LSSI y la LGT. Cabe mencionar que la investigación e instrucción de procedimientos sancionadores se lleva a cabo por la Subdirección General de Inspección de Datos de la AEPD, pero nos referiremos indistintamente a la AEPD en lo que sigue.

1.3.1. Actuaciones previas

El RLOPD regula la posibilidad de realización de actuaciones previas por parte de los agentes de la AEPD, con la precisa finalidad de determinar si existen antecedentes que justifiquen el inicio de un procedimiento sancionatorio[23]. La AEPD tiene expresa habilitación legal para llevar a cabo las actuaciones previas de oficio, o bien por denuncia, o por requerimiento razonado de otro órgano público. Para llevar a cabo su cometido, los agentes de la AEPD cuentan con potestades para recabar información, exigir exhibiciones de documentos y datos, inspeccionar equipos y requerir la ejecución de tratamiento o programas de gestión respecto de los ficheros investigados, pudiendo acceder al lugar donde éstos se encuentren ubicados. Las inspecciones realizadas deben concluir con el levantamiento de un acta de inspección donde se deja constancia de las gestiones o acciones practicadas durante la inspección, de la cual se deja copia al inspeccionado.

Una vez finalizadas las actuaciones previas, éstas deben someterse a la consideración del Director de la AEPD, el cual deberá decidir si existen antecedentes que justifiquen el inicio de un procedimiento sancionatorio o no[24]. En caso negativo, se procede al archivo de los antecedentes, notificando de ello al investigado y al denunciante, si lo hubo. En caso de apreciarse antecedentes que justifiquen la formulación de una imputación contra el investigado, el Director acordará el inicio del procedimiento sancionador.

---

[23] Artículo 120 RLOPD. Excediendo el ámbito propuesto para este trabajo, cabe tener presente una cuestión que no podremos desarrollar aquí, consistente en la pregunta por la naturaleza de estas actuaciones previas: ¿forman parte del procedimiento administrativo sancionador, o bien son actuaciones ajenas al procedimiento, que sirven de antecedente o dato para la posterior iniciación del procedimiento? La pregunta es relevante, por cuanto ella determina si respecto de estas actuaciones previas, el investigado podrá ejercer los derechos de información, oposición e impugnación que los procedimientos administrativos típicamente confieren al interesado; o bien son actuaciones materiales desformalizadas, desprovistas de los estándares de garantía procedimental exigibles a las actuaciones formales (ello, sin perjuicio de acciones cautelares que puedan proceder). También es relevante, por ejemplo, a efectos del artículo 121 RLOPD, pues si no forman parte del "procedimiento", no procedería en esta etapa la inmovilización de ficheros contemplada en esa norma para "cualquier etapa del *procedimiento*". Al parecer, se trataría de actuaciones que tienen lugar "extramuros" del procedimiento sancionador propiamente dicho, cuya finalidad no va más allá de una apreciación acerca de si, efectivamente, se han producido o no los hechos de que se tiene noticia, de modo tal de concluir si hay antecedentes razonables para iniciar el procedimiento. Cfr. Montoya Martín, Encarnación (2008). *Consideraciones sobre las Actuaciones Previas y su Incidencia en el Procedimiento Administrativo Sancionador y en las Garantías del Administrado*. Disponible en: <http://89.248.100.178/da/upload/280-9.pdf> [Consulta: 25 septiembre 2011].

[24] Artículo 126 RLOPD.

Cabe considerar que el RLOPD establece un límite temporal para la práctica de actuaciones previas, de doce meses contados desde la recepción de la respectiva denuncia o requerimiento razonado o, si la actuación previa es oficiosa, contados desde la fecha en que la AEPD haya acordado su realización. El vencimiento de este plazo sin que se haya acordado y notificado el inicio del procedimiento sancionador resulta en la caducidad de las actuaciones previas.

Finalmente, debemos destacar el artículo 49 LOPD en relación con el artículo 121 RLOPD, los cuales disponen que, tratándose de las infracciones catalogadas como muy graves en la LOPD, consistentes en la utilización o cesión no autorizada de datos de carácter personal en los que se impida el ejercicio o se atente de modo grave contra derechos fundamentales, el Director de la AEPD tiene la facultad para, en cualquier estado del procedimiento, ordenar el cese inmediato en la utilización de los datos personales. Si el requerimiento del Director es desatendido, éste puede ordenar la inmovilización de los ficheros.

1.3.2. El procedimiento sancionador

El artículo 127 del RLOPD regula el contenido formal y sustantivo del acuerdo de iniciación del procedimiento sancionador, estableciendo requisitos que apuntan a una adecuada identificación del investigado, información sobre la posibilidad de ejercer derechos en el procedimiento, indicación de medidas provisionales que puedan haberse adoptado, y una clara indicación de los hechos que se imputan, su posible calificación jurídica y las sanciones asociadas; sin perjuicio –indica el mismo artículo– de lo que resulte de la instrucción[25].

Con el acuerdo de instrucción del procedimiento sancionador se abre la etapa de investigación formal, en la cual la AEPD cuenta con amplias atribuciones de investigación y requerimiento de información. La investigación culminará con una resolución de la AEPD que dará por establecida la comisión de una infracción, aplicando la sanción correspondiente; o bien absolverá al investigado, archivando los antecedentes.

La duración del procedimiento sancionador dependerá de si se trata de un procedimiento de sanción bajo la LOPD, la LSSI o la LGT. En el caso de la LOPD, su duración máxima es de seis meses[26], plazo que se computa desde la fecha de dictación del acuerdo de instrucción del procedimiento sancionatorio, hasta la fecha

[25] Esta última posibilidad –que la instrucción resulte en una sanción por hechos distintos a los imputados, o una distinta calificación jurídica– denota que no se exige congruencia entre hechos investigados, imputación y resolución del procedimiento. Esta circunstancia puede eventualmente impactar negativamente sobre la posibilidad de levantar una adecuada defensa en el procedimiento sancionador, toda vez que las imputaciones formuladas determinan la estrategia de defensa, es decir, determinan frente a qué "debe hacerse frente" y, sin embargo, habiendo formulado una defensa contra una imputación específica, se puede resultar sancionado por una causal diversa, no prevista y por ello no adecuadamente defendida.

[26] Artículo 48 LOPD.

de notificación de la decisión terminal en el mismo. El vencimiento de dicho plazo sin que se haya dictado y notificado una resolución expresa, produce la caducidad del procedimiento y el archivo de los antecedentes[27].

1.3.3. Recursos

Ni la LOPD ni el RLOPD regulan un régimen específico de impugnación de las decisiones de la AEPD en el ejercicio de sus potestades sancionatorias. Consecuentemente, en este punto reciben plena aplicación las normas generales sobre procedimientos administrativos vigentes en España. Por ello, contra la resolución de la AEPD que ponga fin a la vía administrativa[28], los interesados podrán interponer un recurso de reposición ante el Director de la AEPD dentro del plazo de un mes a contar desde la notificación de la resolución de término[29]; o un recurso contencioso administrativo ante la Sala de lo Contencioso-Administrativo de la Audiencia Nacional[30], dentro del plazo de dos meses a contar desde la notificación de dicha resolución de término.

1.4. Régimen de infracciones y sanciones aplicables

En la sección 1.3. anterior revisamos brevemente los aspectos generales sobre la sustanciación del procedimiento sancionador por la AEPD. Corresponde revisar, ahora, el catálogo de infracciones y sanciones que contempla el Título VII de la LOPD.

Partiremos primero por una breve revisión de las sanciones, pues la primera cuestión que llama la atención de la LOPD en este aspecto es el establecimiento de un régimen diferenciado de sanciones, según se trate de ficheros de los que sean responsables las Administraciones Públicas, o bien otros individuos (privados)[31]. En efecto, mientras que para personas o entidades que no pertenecen a las Administraciones Públicas la principal sanción por infracciones a la LOPD es la sanción pecuniaria[32], las cuales pueden alcanzar sumas relevantes[33], las sanciones previstas para

[27] Artículo 128 RLOPD.

[28] Artículo 48.2 LOPD.

[29] Artículo 116 de la Ley Nº 30/1992, 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

[30] Artículos 25 y 46.1 de la Ley Nº 29/1998, 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, y sección 5 de la disposición adicional cuarta de la misma ley.

[31] Idéntica situación ocurre en el Proyecto de Reforma chileno, según veremos en la sección Nº 3: multas para privados, sumarios administrativos para órganos públicos.

[32] Artículo 45 LOPD.

[33] Las sanciones pecuniarias máximas pueden alcanzar los € 600.000, motivo más que suficiente para que una PYME o una empresa de mediano tamaño ajusten su actuar a la LOPD, y las grandes empresas tomen

las Administraciones Públicas[34] no contemplan sanciones de carácter pecuniario para el organismo o servicio de que se trate, ni para el funcionario responsable. Cuando la infracción se comete respecto de un fichero que corresponda a las Administraciones Públicas, el Director de la AEPD dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción; y adicionalmente podrá proponer la iniciación de actuaciones disciplinarias, si procedieran, cuya instrucción y eventual sanción competen al organismo de que se trate.

Creemos que esto genera en el sector público un incentivo al cumplimiento más bajo que en el sector privado, toda vez que una infracción a la LOPD por el primero no generará mayores consecuencias, además de un (posible) impacto sobre la imagen del organismo o servicio, y (eventualmente) una sanción disciplinaria para los funcionarios responsables por la infracción. Por otro lado, si hipotéticamente existieran sanciones pecuniarias para las Administraciones Públicas, se produciría el sinsentido de que se le aplica una multa al Estado, que iría a favor del propio Estado; y tratándose de organismos o servicios con patrimonio propio, se privaría de parte de su presupuesto público a un organismo o servicio en razón de la infracción cometida, que originalmente estaba destinado para ejecutar la función pública que se le encomienda, en detrimento de dicha función. A la luz de lo anterior, podrían preferirse soluciones intermedias, donde la AEPD pueda imponer, directamente y sin mediar nuevo procedimiento disciplinario, multas personales a los funcionarios públicos personalmente responsables de las infracciones graves, cuando éstos no hayan representado previamente las posibles infracciones, lo que generaría mayores incentivos al cumplimiento en el sector público.

En cuanto al catálogo de infracciones establecido por la LOPD, cabe consignar que el régimen de infracciones, a diferencia de las sanciones, es común tanto a privados como a las Administraciones Públicas. Existen tres categorías de infracciones, calificadas como leves[35], graves[36] y muy graves[37]. No podremos extendernos sobre las mismas, pero debemos destacar que constituyen infracciones muy graves la recogida de datos en forma engañosa y fraudulenta; la comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas; tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales; no atender u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición, e incumplir el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.

asimismo en consideración el debido cumplimiento de la normativa sobre protección de datos. La (amenaza de) sanción pecuniaria se convierte así en un importante elemento disciplinador del mercado.

[34] Artículo 46 LOPD.

[35] Artículo 44.2.

[36] Artículo 44.3.

[37] Artículo 44.4.

1.5. Prescripción

Las infracciones muy graves prescriben en el plazo de tres años, las graves en dos años y las leves en un año[38]. El plazo de prescripción se computa desde el día en que la infracción se hubiera cometido, y se interrumpe por la iniciación, con conocimiento del interesado, del procedimiento sancionador, reanudándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor.

2. Contrapunto: El Proyecto de Reforma chileno

2.1. ¿Quién conocerá de las infracciones a la Ley Nº 19.628? Órganos competentes y procedimientos

El primer punto que llama la atención respecto del Proyecto de Reforma es que existen procedimientos diferenciados y organismos competentes diversos según se trate de procedimientos contra organismos públicos o privados, y según la finalidad del procedimiento. Y, en todos los casos, el procedimiento se inicia bajo el principio de rogación, careciendo los diversos organismos de potestades oficiosas de control, inspección y sanción de infracciones a la Ley Nº 19.628, poniendo de cargo de los particulares el inicio de la persecución de infracciones (y los costos) para proteger un bien jurídico de relevancia pública, y que incide sobre otros derechos fundamentales. Ello contrasta diametralmente con la legislación española (y las legislaciones europeas en general), toda vez que ésta establece un ente administrativo independiente de control y sanción con potestades oficiosas, según hemos visto.

De este modo, si el reclamo del particular se dirige contra organismos públicos, el órgano de control competente al cual debe dirigirse la reclamación será el Consejo Para la Transparencia[39] (en adelante "CPLT"), el reclamo se sustanciará de conformidad con el procedimiento contemplado en la Ley Nº 19.880, y las sanciones aplicables y responsabilidades administrativas de los funcionarios se determinarán por el CPLT, de conformidad con lo dispuesto en la letra (m) del artículo 33 de la Ley Nº 20.285. Es decir, el CPLT deberá requerir del órgano de que se trate el inicio de un sumario administrativo para perseguir responsabilidades administrativas. A los organismos contemplados en la letra (k) del artículo 2 del Proyecto de Reforma se aplican los procedimientos contemplados en sus propias leyes orgánicas. Cuando el órgano reclamado sea el propio CPLT, la Contraloría General de la República podrá incoar el respectivo procedimiento disciplinario y establecer sanciones.

[38] Artículo 47 de la LOPD.

[39] Artículo 16.A Proyecto de Reforma.

Debemos tener presente aquí que los Consejeros Directivos del CPLT son designados por el Presidente de la República[40], y son removidos por la Corte Suprema, a requerimiento del Presidente de la República, de la Cámara de Diputados mediante acuerdo adoptado por simple mayoría, o a petición de diez diputados, por "*incapacidad, mal comportamiento o negligencia manifiesta en el ejercicio de sus funciones*"[41]. También se contemplan causales legales de cesación del cargo, en la misma norma.

Si el reclamo se dirige contra una entidad privada, en cambio, el reclamo deberá interponerse ante el juez de letras en lo civil que corresponda al domicilio del presunto infractor[42], órgano jurisdiccional que será competente tanto para aplicar sanciones, como para conocer de eventuales acciones indemnizatorias (sobre las cuales tiene competencia exclusiva en todo caso).

Sin perjuicio de poder recurrir ante el tribunal civil, el afectado podrá recurrir ante el Servicio Nacional del Consumidor para que éste promueva un entendimiento voluntario con el supuesto infractor, que se sustancia de conformidad con lo dispuesto en el artículo 58.f de la Ley Nº 19.496. Si el entendimiento no prospera, puede en todo caso recurrir al tribunal civil, de conformidad con lo expuesto en el párrafo precedente.

2.1.1. Primera Crítica: Protección de derecho fundamental depende enteramente de privados. Multiplicidad de órganos competentes y de procedimientos. Falta de independencia del control público

En mi opinión, resulta tremendamente inconveniente poner de cargo de los individuos la protección del derecho a la autodeterminación informativa y la protección de la privacidad, que es exactamente lo que se hace cuando son éstos quienes deben iniciar y sustanciar los reclamos ante el CPLT (aportando además los antecedentes necesarios), o presentar sus reclamaciones ante un tribunal civil y tramitar un juicio para obtener una eventual sanción por la infracción, con los costos asociados a ello. Esta decisión resulta inconveniente, por cuanto el costo individualmente considerado para un particular de una infracción cometida en su contra con frecuencia será menor que el costo económico y de tiempo asociado a perseguir las responsabilidades, lo que desincentiva fuertemente el inicio de investigaciones. Además, el particular normalmente estará en desventaja, tanto desde la perspectiva de la información de que dispone, como de la (falta de) capacidad técnica para participar con efectividad de un procedimiento que normalmente involucrará discurrir sobre complejos aspectos tecnológicos aparejados a las infracciones. Con frecuencia será imposible para un particular sustanciar y obtener resultados (o siquiera detectar infracciones) frente a empresas de tecnología de

[40] Artículo 36, Ley Nº 20.285.

[41] Artículo 37, Ley Nº 20.285.

[42] Artículo 16.B Proyecto de Reforma.

la información altamente especializadas, que cuentan con sofisticados sistemas y recursos tecnológicos. Esta situación es como si el control y sanción de infracciones en el contexto de los mercados financieros dependiera exclusivamente de que los privados detectaran e iniciaran las acciones correspondientes; o como si el cumplimiento de las normas de tránsito dependiera exclusivamente de que los propios privados iniciaran acciones en contra de los infractores: la persecución y sanción de infracciones resulta, sencillamente, ilusoria.

En segundo término, la dualidad entre órganos/procedimientos públicos (CPLT y Ley Nº 19.880) y órganos/procedimientos privados (juez civil y sumario especial) previsiblemente generará una disparidad de criterios jurisprudenciales en cuanto al sentido, alcance y finalidades de la Ley Nº 19.628, habida cuenta de sus diferentes estructuras institucionales, procedimientos, entrenamiento, especialidad y "culturas" jurídicas. Donde se presente disparidad de criterios frente a situaciones esencialmente idénticas, se atenta contra la igualdad ante la ley. Con todo, tanto las resoluciones del CPLT como las del tribunal civil son revisables por la Corte de Apelaciones respectiva, aunque las primeras lo son por vía de una reclamación de ilegalidad (un examen esencialmente de derecho) y las segundas por medio de un recurso de apelación[43], recurso de amplio alcance que posibilita pronunciarse sobre todas las cuestiones de hecho y derecho debatidas y que se propongan como fundamento del recurso). El recurso de apelación se concede siempre en ambos efectos (artículo 16.B.k).

En tercer lugar, no se ha contemplado la posibilidad para ninguno de los órganos administrativos de control de querellarse cuando los ilícitos que involucran datos personales que revistan carácter penal[44].

Finalmente, una cuestión particularmente sensible referida a los reclamos contra el sector público viene dada por la gran injerencia que tiene el Poder Ejecutivo sobre el nombramiento y remoción de los Consejeros Directivos del CPLT, configuración institucional que impacta directamente sobre la independencia orgánica del mismo[45], condición esencial para un óptimo cumplimiento de la misión de protección del individuo frente al Estado. Esta situación no sólo debe revisarse respecto de la protección de datos personales, sino también en su faceta de órgano de control de la normativa sobre transparencia pública.

[43] Artículo 16.B.i. Proyecto de Reforma.

[44] Véase, por ejemplo, el artículo 4 de la Ley Nº 19.223, que sanciona ilícitos penales relativos a la informática.

[45] El tema es de la mayor importancia, y una inadecuada solución en la regulación sobre este punto puede poner en entredicho no sólo la independencia del órgano, sino también la confianza general de la ciudadanía en la institucionalidad concernida. Ejemplos de ello fueron dos casos sobre transparencia pública que enfrentaron al CPLT con intereses que involucran directamente a La Moneda (uno de ellos involucra nada menos que a la esposa del Presidente de la República), y que ahora generan dudas en torno al proceso de renovación de Consejeros del CPLT. Disponible en: <http://ciperchile.cl/2011/10/06/los-ultimos-rounds-del-presidente-del-consejo-para-la-transparencia-con-la-moneda/> [Consulta: 9 octubre 2011].

En suma, nuestro primer orden de críticas apunta a que existen diversos entes competentes (CPLT, Sernac, tribunales comunes y, excepcionalmente, la Contraloría General de la República), cuyas naturalezas, funciones y organización son por completo disímiles, y una multiplicidad de procedimientos (Ley Nº 19.880, sumario especial, entendimiento voluntario y procedimiento de su propia ley orgánica para ciertos órganos públicos). Todo lo cual propende a una protección fragmentaria del bien jurídico, a una disparidad de criterios, y a mayores costos para los privados en la protección de un bien jurídico que trasciende con creces el ámbito de lo meramente privado. Dirigimos una especial crítica a la disminuida independencia orgánica del CPLT, emanada de la gran injerencia que tiene el Poder Ejecutivo sobre el nombramiento y remoción de sus Consejeros.

2.1.2. Segunda Crítica: Funciones contrapuestas del CPLT. Máxima transparencia versus protección de datos personales

En otro orden de cuestiones, resulta complejo encomendarle al CPLT una función que, a mi juicio, representaría una permanente tensión y oposición con su misión institucional por excelencia: la transparencia pública. Y es que el problema de fondo que pretende zanjar cualquier regulación sobre datos personales radica en trazar un equilibrio razonable entre intereses legítimos divergentes. Como elocuentemente pregunta RAJEVIC, "[e]l conflicto, entonces, es inevitable, ¿qué principios aplicaremos cuando nos enfrentemos a esta intersección? ¿El deber de resguardar la confidencialidad de los datos personales o el derecho de las personas a acceder a la información pública? ¿A quién le encargaremos resolver este conflicto? ¿A una sola autoridad administrativa que maneje ambos temas o a los tribunales de justicia?"[46]. Según el mismo autor, cerca de la cuarta parte[47] de las decisiones de fondo dictadas por el CPLT durante el primer trimestre 2011 tuvieron que ver con datos personales, por lo cual una respuesta adecuada a estas interrogantes resulta apremiante.

Se trata entonces –como ponía de relieve JIJENA más de una década atrás– de lograr un equilibrio adecuado entre el derecho a la intimidad protegido en el artículo 19 Nº 4 de la Constitución, y el derecho a la información consagrado en el artículo 19 Nº 12[48]. De balancear el derecho a la autodeterminación informativa con el derecho

[46] RAJEVIC MOSLER, Enrique (2011). "Protección de datos y transparencia en la administración pública chilena: Inevitable y deseable ponderación". En: *Reflexiones sobre el Uso y Abuso de los Datos Personales en Chile*. Expansiva, Santiago, p. 137. Disponible en: <http://www.redrta.org/Proteccin%20de%20Datos/Chile-Protecci%C3%B3n%20de%20datos%20y%20transparencia%20en%20la%20administraci%C3%B3n%20chilena.pdf> [Consulta: 13 noviembre 2011].

[47] Ibíd., p. 150.

[48] *Vid.* JIJENA LEIVA, Renato (2001). "La Ley Chilena de Protección de Datos Personales. Una Visión Crítica desde el Punto de Vista de los Intereses Protegidos". En: *Tratamiento de Datos Personales y Protección de la Vida Privada*, WAHL SILVA, Jorge (Edit.), Cuadernos de Extensión Jurídica, Universidad de los Andes, Nº 5, Santiago, pp. 86-88.

a la información, en buenas cuentas. Si esa tensión debe ser resuelta por un único ente, conceptual y funcionalmente diseñado para la misión de transparencia de la información, la efectiva protección de los datos personales peligra.

En efecto, una parte importante de la información que obra en poder del Estado está constituida por datos personales; y dada la amplísima definición de lo que constituye "información pública" a la luz de la Ley Nº 20.285, nos mostramos escépticos ante los estándares de resguardo de los datos personales que exhibirá (y que ha exhibido hasta ahora) el CPLT de cara a su misión de transparencia pública, lo que supone la ponderación de valores en conflicto por parte de un único órgano, sin que nadie "fiscalice" o "discipline" la ponderación que efectúa[49]. Esto lo constituye en un verdadero "bicéfalo" a cargo de funciones contrapuestas, donde la experiencia nos dice que la función de transparencia pública –para la cual fue específicamente diseñado– tiende a desplazar a la protección de datos personales a un lugar muy secundario[50]. Y eso, de suyo complejo para un adecuado resguardo de los derechos fundamentales, en un contexto donde hasta hace poco el 63% de los ficheros que están en custodia del sector público se refieren a bases que contienen datos personales de beneficiarios de los mismos, y donde sólo el 21% de los organismos públicos señala tener políticas de seguridad respecto de esos datos, es muy grave[51].

2.2. Procedimiento sancionatorio: Impulso procesal (y costos) de cargo de los afectados

A diferencia de la AEPD, ninguno de los diversos entes competentes en el Proyecto de Reforma se encuentra dotado de potestades oficiosas para realizar inspecciones y controles a las entidades públicas y privadas, en carácter de actuaciones previas, como sí lo está la AEPD. El sistema descansa, como dijimos anteriormente, en que los individuos decidan que los costos de la impunidad son más altos que

[49] De modo análogo a como la Defensoría Penal Pública en Chile funciona como contrapeso institucional, fiscalizador y disciplinador de la actividad persecutora ejercida por el Ministerio Público en materia penal, por ejemplo.

[50] Véase, por ejemplo, comentario de Carlos Reusser sobre el caso "SERVEL". Disponible en: <http://www.elmostrador.cl/opinion/2010/06/09/la-traicion-del-consejo-de-la-transparencia/> [Consulta: 2 octubre 2011]. "*…el Consejo para la Transparencia aspira también en constituirse en la autoridad de protección de datos de Chile, transformándose en un imparable ente bicéfalo que ya está atentando contra los derechos de las personas*". Véase también comentario de Renato Jijena. Disponible en: <http://www.leydetransparencia.gob.cl/multimedia/prensa/transparencia-no-datos-personales> [Consulta: 2 octubre 2011].

[51] Véase estadísticas y comentarios de Fundación ProAcceso referidos al caso "La Polar" y el mal uso de los datos personales de millones de chilenos contenidos en bases de datos de Fonasa. Disponible en: <http://www.proacceso.cl/contenido_general/tr_fico_de_datos_personales_en_chile_la_ley_de_la_selva> [Consulta: 2 octubre 2011]. Además, puede consultarse el estudio de la misma fundación Fundación ProAcceso (2011). *Estudio de Protección de Datos Personales en el Servicio Público*. Disponible en: <http://www.proacceso.cl/noticia/estudio_de_pro_acceso_revela_deficiencias_en_la_administraci_n_de_bases_de_datos_personales_> [Consulta: 2 octubre 2011].

las lesiones que individualmente experimenten en sus derechos, e interpongan las acciones correspondientes.

Tratándose del procedimiento ante el CPLT, en general, nos parece que las reglas son apropiadas (nos referimos al procedimiento establecido en la Ley Nº 19.880), en cuanto propenden a minimizar las formalidades y establecen instancias apropiadas de instrucción, contradicción e impugnación, todo ello bajo plazos acotados. En cuanto a la prescripción de las infracciones, se ha optado por establecer un plazo general de tres años para todo tipo de infracción (artículo 31 Proyecto de Reforma). Llama la atención que dicha norma indica que la prescripción se interrumpe por el ejercicio de la acción por el titular ante el juez civil, o mediante reclamo ante el Servicio Nacional del Consumidor, pero nada dice acerca de la presentación de un reclamo ante el CPLT. ¿No interrumpe la prescripción la presentación de un reclamo ante el CPLT? Nos parece que esto es solamente una omisión inadvertida en el proyecto, que deberá corregirse[52].

En cuanto al procedimiento ante los tribunales civiles (es decir, contra entidades privadas), éste mantiene la estructura general de un juicio sumario, vale decir, presentación de reclamo, contestación (dentro de 5º día), audiencia de prueba y sentencia; con las modificaciones que en el artículo 16.B del Proyecto de Reforma se indican, y con aplicación supletoria del juicio sumario previsto en el Libro III del Código de Procedimiento Civil.

En general, las modificaciones que contempla el Proyecto de Reforma con respecto al procedimiento judicial actualmente vigente[53], tienen por finalidad sustanciar el procedimiento de manera más expedita, por la vía de imponerle al juez el deber de proveer el reclamo presentado en 24 horas[54], el que se notifica por correo electrónico al reclamado o por cédula si no cumplió con su deber de publicar un correo electrónico en su página web, y se establecen plazos acotados de discusión y sentencia. Contra la sentencia definitiva sólo podrá interponerse recurso de apelación y solicitud de aclaración, rectificación o enmienda. Contra la sentencia de segunda instancia no procederá recurso de casación, pero nada se dice acerca del recurso de queja o el recurso extraordinario de revisión. Nada se dice tampoco acerca del régimen de impugnación de sentencias interlocutorias

[52] Por otra parte, podría decirse que si la intención era establecer la interrupción de la prescripción en general con una presentación a cualquiera de los entes competentes, el legislador no habría individualizado ante quiénes dicha presentación produce la interrupción de la prescripción. Sin embargo, no se advierte el sentido o finalidad de exceptuar a las reclamaciones ante el CPLT de los efectos de la interrupción de la prescripción, por lo cual esta lectura no nos convence.

[53] Dispone actualmente el artículo 23 de la Ley Nº 19.628 que "…*las infracciones no contempladas en los artículos 16 y 19, incluida la indemnización de los perjuicios, se sujetarán al procedimiento sumario. El juez tomará todas las providencias que estime convenientes para hacer efectiva la protección de los derechos que esta ley establece. La prueba se apreciará en conciencia por el juez*".

[54] Aunque no se establece ninguna sanción o mecanismo para obtener el cumplimiento efectivo de esta disposición, en caso de que el juez no cumpla.

u otro tipo de resoluciones, con lo cual no cabría sino entender que se aplican supletoriamente las reglas del Código de Procedimiento Civil al respecto.

2.2.1. Crítica: el procedimiento sigue siendo judicial. Desesperadamente judicial

Creemos que vale la pena reiterarlo: el procedimiento depende enteramente de que los individuos decidan enfrentar los costos en términos de tiempo y dinero que implica sobrellevar un litigio civil. No existe nada en la regulación propuesta análogo a las facultades para llevar a cabo actuaciones previas por parte de la AEPD. Queda así entregado a manos de particulares el control, fiscalización y disciplina de los entes privados en el tratamiento que éstos efectúen de datos personales, lo cual obviamente deja el control en entredicho. Dicha situación, además, restringe la legitimación activa, puesto que sin normas especiales que regulen el punto, solamente podrá interponer un reclamo quien tenga un derecho involucrado en el asunto (en oposición a una mera expectativa), de modo tal que si X toma conocimiento de una infracción cometida en contra de Y, no queda más que esperar que el propio Y se decida a tomar cartas en el asunto.

Esto no resulta problemático tratándose de derechos pecuniarios de carácter disponible, cuyo resguardo queda entregado a la voluntad privada; pero resulta muy problemático tratándose del resguardo de un derecho fundamental del cual depende, a su turno, el respeto de otros derechos fundamentales, y donde con frecuencia no habrán intereses económicos relevantes en juego, pero sí el ejercicio de derechos fundamentales, intereses "morales" o lesiones de carácter extrapatrimonial. Por lo demás, huelga decir que quienes podrán acceder a este mecanismo de protección serán quienes dispongan de recursos suficientes, quedando desprotegidos quienes no puedan costear el acceso a tribunales[55].

Por otra parte, el Proyecto de Reforma deja una serie de cuestiones indefinidas sobre el procedimiento judicial: ¿Cuándo se entiende practicada y cómo se certifica la notificación por correo electrónico? La falta de claridad sobre el punto deja expuesto todo litigio a un incidente de nulidad de lo obrado por falta de emplazamiento válido. ¿Cuál es la sanción procesal para el ente privado por no publicar la casilla de correo electrónico en el sitio web? El artículo 16.B.d. del Proyecto de Reforma establece que si no publica la dirección de correo electrónico, deberá ser notificado por cédula. Vale decir, resulta más conveniente para el ente inescrupuloso

[55] Por diversas razones que no es del caso tratar aquí, estimo insuficiente contestar a esta última objeción aduciendo que quienes no puedan solventar estos costos pueden reclamar el beneficio del artículo 591 del Código Orgánico de Tribunales y ser asesorados por la Corporación de Asistencia Judicial, encontrándose esta última en una posición institucional débil para gestionar rápida y efectivamente las causas que ingresan a su conocimiento.

no publicar su correo electrónico, de modo tal de elevar los costos y tiempos del emplazamiento, disuadiendo eventuales presentaciones[56].

Creemos conveniente, además, adecuar la regulación de las medidas cautelares contenida en el Código de Procedimiento Civil, de modo tal de adaptarlas a las necesidades propias de esta materia; nada de lo cual es abordado por el Proyecto de Reforma. Persiste en el Proyecto la necesidad de notificar por cédula la sentencia, en circunstancias que incluso el emplazamiento podía efectuarse vía correo electrónico, lo que sólo significa más costos y pérdida de tiempo para los individuos en la tramitación del juicio.

Todo lo anterior contrasta con el procedimiento sancionador sustanciado ante la AEPD, desformalizado, concentrado, y donde el impulso corresponde a la propia AEPD, dotada de los recursos y conocimientos especializados para ello.

Adicionalmente, queremos solamente mencionar que no obstante todas las reformas procedimentales que se introducen por vía del artículo 16.B del Proyecto de Reforma, con la finalidad de hacerlo más expedito, persiste el hecho concreto de que los tribunales civiles están imbuidos de una determinada cultura judicial, una especial forma de hacer las cosas, verdaderas "costumbres procesales" contra las cuales resulta muy difícil imponer cambios sustantivos. La degeneración del juicio sumario del Código de Procedimiento Civil –proyectado como un juicio expedito y oral en su regulación– es un muy buen ejemplo de lo poderosas que pueden resultar las costumbres y hábitos dentro de una determinada "subcultura" funcionaria, las que terminaron haciendo de este procedimiento un juicio esencialmente escrito y de dilatada tramitación. Incluso por este solo aspecto "cultural" (a falta de mejor término), habría resultado deseable remover el conocimiento de infracciones a la Ley Nº 19.628 de los tribunales civiles, radicándola en un ente diverso y especializado.

En buenas cuentas, entregar la misión de tutela de derechos fundamentales a un juez civil significa poner exclusivamente sobre los hombros del individuo los costos, dificultades e impulso procesal para sustanciar un litigio, y hacerlo bajo reglas y ante tribunales en exceso formalizados y legicentristas, en circunstancias de que se trata de la protección de un bien jurídico fundamental que excede con creces del interés meramente privado del afectado. Que no se corresponde con los conflictos "típicos" que los juzgados civiles acostumbran procesar (i.e. contratos y cobranzas); que normalmente involucrará aspectos altamente técnicos enfrentando a potenciales infractores altamente especializados; y que requiere de tutela eficaz y

[56] La omisión en la publicación de la casilla de correo electrónico es catalogada como una infracción leve, según el artículo 23 literal (e) del Proyecto de Reforma. Pero, insistimos, si el organismo que omite la publicación de la casilla de correo electrónico es un ente privado, el procedimiento para reclamar de dicha infracción es… ¡judicial! Vale decir, el privado deberá sobrellevar de todos modos los costos de un litigio (sin perjuicio de que, al finalizarlo exitosamente, pueda, en teoría, recobrar al menos parte de lo gastado vías costas procesales).

sobre todo expedita, algo en que nuestros tribunales civiles sencillamente no son buenos[57].

En suma, concordamos con Cerda en que las limitaciones propias del objeto, oportunidad e impulso de la tutela jurisdiccional en sede civil la tornan insuficiente para hacer frente a los riesgos y especiales características y formas de comisión del tratamiento indebido de datos, no sólo para los individuos concernidos, sino para el sistema democrático más ampliamente considerado[58].

2.3. Catálogo de infracciones y sanciones

Al igual que la LOPD, el Proyecto de Reforma contempla en su artículo 23 un catálogo único de infracciones, que se clasifican en infracciones leves, graves y gravísimas, lo cual incide sobre la entidad de las sanciones asociadas.

De la comparación de las normas, llama la atención la menor gravedad que la norma chilena asigna al tratamiento ilegítimo de datos o sin consentimiento del titular, en general (infracción grave, 23.a, e, i, j) por comparación con la norma española (artículo 44.4 LOPD) que clasifica tales infracciones como muy graves.

En cuanto a las sanciones existen mayores diferencias con la normativa española. La norma chilena establece como principal sanción la multa (artículo 24 Proyecto de Reforma) y también distingue entre organismos públicos y privados a efectos de la sanción aplicable. Valgan aquí las observaciones que formulamos en la sección 2.5 sobre esta diferenciación, y la sugerencia asociada a dicha observación.

Ahora, en cuanto a las diferencias, llama la atención que la entidad de las sanciones pecuniarias es más bien baja[59]. Si bien, en general, se levantan consideraciones en torno a los principios que deben inspirar al derecho administrativo sancionador, trayendo a éste un principio propio del Derecho Penal clásico como es la *proporcionalidad de la sanción* concernido como estaba por la libertad y la integridad física y psíquica de la persona, debe considerarse aquí que el catálogo de sanciones es sólo secundariamente –casi por añadidura– punitivo. A mi juicio,

[57] En los tribunales civiles de Santiago, obtener una sentencia definitiva en juico ordinario demora 821 días en promedio, mientras que obtener una sentencia definitiva en juicio sumario demora 226 días en promedio. Fuente: Centro de Estudios de Justicia de las Américas (CEJA) (2011). *Estudio de análisis de trayectoria de las Causas Civiles en los Tribunales Civiles de Santiago*. Informe Final, Santiago, mayo, pp. 22-28. Sin embargo, el promedio en juicio sumario es "engañoso", toda vez que se tramitan conforme a dicho procedimiento una serie de materias de muy rápida resolución, tales como la designación de árbitros, por lo cual dicho promedio podría ser mayor en procedimientos contenciosos de tutela de derechos fundamentales.

[58] Cfr. Cerda Silva, Alberto (2006). "Mecanismos de Control en la Protección de Datos en Europa". *Ius et Praxis*, año 12, Nº 2, 2006, p. 237.

[59] Como máximo, 1.000 UTM, considerando además que de acuerdo al propio artículo 24, para efectos del cálculo de la multa, cada "grado" se divide en dos, correspondiendo siempre el rango inferior a una infracción que se comete por primera vez, y el rango superior, de acuerdo a las circunstancias agravantes y condiciones especiales de aplicación de las multas que establece esta ley. Adicionalmente, según explicamos, se contemplan varias atenuantes y mecanismos alternativos para evitar o atenuar la sanción.

la finalidad del establecimiento de sanciones pecuniarias en este ámbito es uno de *disciplina* del mercado y del Estado. Por ello, no sirve –a efectos de proteger el bien jurídico– que la sanción sea proporcional a la infracción (cuestión que sí es muy relevante tratándose de la libertad personal), pues el juicio de proporcionalidad invita a realizar consideraciones acerca del beneficio/utilidad de incurrir en la infracción y pagar la multa versus cosechar los beneficios de tal conducta. Más bien, la sanción debiera ser *desproporcionadamente* mayor que la infracción asociada, de modo tal de inhibir al mercado y al Estado, disciplinándolos, y dificultar, por la vía de la eventual sanción, que la ponderación beneficio/infracción en el tratamiento de datos sea resuelta a favor de lo primero, el "beneficio" o ganancia asociada a la conducta ilícita.

En esta perspectiva, debemos llamar la atención sobre una serie de medidas que tienden a desplazar o atenuar la responsabilidad de infractores.

Primero, el Proyecto de Reforma establece mecanismos alternativos para resolver infracciones a la ley, que la LOPD no contempla. En particular, establece la posibilidad de configurar una atenuante por auto-denuncia, presentando un acuerdo reparatorio al Sernac[60], pero la norma no salva con precisión cómo ha de funcionar este mecanismo a la luz de la diferenciación de organismos competentes y de procedimientos, según el infractor sea público o privado, ni el curso de acción a seguir, para el evento de estimarse insuficiente el acuerdo, o no cumplirse. Sería interesante si, además de la atenuante por autodenuncia, se contemplara la posibilidad de una atenuante por delación o delación compensada, esto es, un beneficio para el infractor en caso de que delate a otro infractor ante la autoridad competente y ello conduzca a la aplicación de una sanción para este último; pero, naturalmente, esto requiere que exista una autoridad con potestades de persecución de oficio a efectos de que dicha delación tenga alguna utilidad.

Segundo, se establece una atenuante de responsabilidad en la aplicación de las multas, si el infractor acredita haber cumplido diligentemente con sus deberes de dirección y supervisión para la protección de los datos personales bajo su responsabilidad o tratamiento[61]. Este punto, aisladamente, no parece en sí mismo problemático, en cuanto previsiblemente genera incentivos al cumplimiento. Sin embargo, acto seguido, la norma indica que se entiende cumplido el estándar de diligencia por el hecho de implementar un modelo de organización, administración y supervisión para prevenir la infracción cometida, certificado por una empresa certificadora de cumplimiento. Esto sí parece problemático.

En realidad, el establecimiento de medidas de organización, administración y supervisión debiera ser el estándar exigible, pues tales medidas resultan consustanciales al ejercicio de una actividad en forma respetuosa de los derechos

[60] Artículo 25 Proyecto de Reforma.

[61] Artículo 26.

fundamentales, tanto por entidades públicas como privadas. Luego, la existencia de tal modelo debiera ser sencillamente el estándar exigible, y su ausencia, indicio de negligencia grave. Pero, en la forma propuesta por el Proyecto de Reforma, se establece una presunción *iuris tantum* de diligencia por el hecho de implementar el modelo certificado, trasladando al individuo (pues en ellos recae la persecución de responsabilidades según se plantea en el Proyecto) la carga de derrotar dicha presunción de diligencia, acreditando que el infractor no fue diligente pese a contar con el modelo certificado. En un contexto de asimetría de información y de conocimientos técnicos, lo más probable es que el individuo nunca esté en posición de derrotar tal presunción frente al Estado o a empresas de tecnologías de la información altamente especializadas y operando en campos eminentemente técnicos.

Por otra parte, también se establece la posibilidad de imponer una sanción accesoria de suspensión de las operaciones del registro o base de datos, hasta por un término de seis meses[62], tratándose de infracciones graves o muy graves. Aquí, debiera abrirse el catálogo de posibilidades para que sea el órgano de control quien determine cuáles son la medidas a seguir para poner término a las infracciones y precaverlas en el futuro, de manera análoga a como se establece en la LOPD, pero la norma parece cerrarse a la sola posibilidad de suspensión, con el grave perjuicio que eventualmente ello acarrearía al debido funcionamiento de servicios públicos o emprendimientos cuya suspensión no pueda llevarse a cabo sin grave perjuicio para terceros.

Tercero, para efectos del cálculo de la multa aplicable, cada grado se dividirá en dos, correspondiendo siempre el rango inferior a una infracción que se comete por primera vez, y el rango superior, de acuerdo a las circunstancias agravantes y condiciones especiales de aplicación de las multas que establece el Proyecto; y la reparación otorgada por el infractor al afectado, previo acuerdo entre ambos, será considerada, como una atenuante[63], confundiendo así la reparación de un perjuicio privado con la responsabilidad legal por la infracción de una norma que no mira (únicamente) al interés privado.

En definitiva, el catálogo de sanciones previstas en el Proyecto de Reforma no parece ser suficientemente robusto como para efectivamente conminar al cumplimiento oportuno y efectivo de las normas sobre protección de datos. Si a ello se suman las salidas alternativas para el infractor y la amplia posibilidad de configuración de atenuantes de responsabilidad, puede concluirse que el Proyecto de Reforma, en lo que a sanciones se refiere, está concernido más con el desarrollo razonable de un actividad económica lucrativa, que con la efectiva protección de un derecho fundamental.

[62] Artículo 30.

[63] Artículo 24.

CONCLUSIONES

Mientras que España contempla un órgano de control autónomo, independiente y especializado en materia de protección de datos personales, Chile estaría apostando por una multiplicidad de órganos competentes, con diseños institucionales, formación técnica y misiones muy disímiles; y en el contexto de una decisión explícita por la atomización de la información tratada, en perjuicio de los individuos[64]. No se advierten posibles ventajas de la elección de una institucionalidad fragmentaria[65] y sí muchas desventajas, todas en perjuicio de la protección de los derechos de los individuos. Mención especial merece la elección del CPLT como órgano de control de entes públicos, en circunstancias que su diseño y misión por excelencia es la tutela de un bien jurídico con frecuencia antagónico a la protección de datos personales: la transparencia pública. Según comentamos en 2.1.2., esta última función tiende a desplazar la primera.

Mientras que España establece potestades oficiosas de control, instrucción y sanción para la AEPD, sin perjuicio de que el individuo pueda accionar en sede jurisdiccional para obtener resarcimiento patrimonial, Chile descansa esencialmente sobre el impulso de los particulares para poner en marcha los mecanismos institucionales (administrativos y judiciales) de protección de datos personales, y descansa sobre la decisión, capacidad técnica y económica de dichos particulares para sustanciar procedimientos, ya sea contra la Administración del Estado o contra empresas o individuos especializados en tecnologías de la información. La asimetría entre particulares, por un lado, y Estado y empresas de tecnología, por otro, pone en entredicho la efectividad de los mecanismos de protección de datos personales propuestos en la reforma.

El régimen de sanciones, por otra parte, nos parece insatisfactorio por las razones que comentamos en el apartado correspondiente; y, en general, considerando su monto, atenuantes y salidas alternativas, parecen bastante "blandas" por comparación con la LOPD, lo que hace dudar de su capacidad para conminar al cumplimiento efectivo de la ley y al respeto por los derechos fundamentales de las personas.

Sólo a efectos de contrastar, cabe mencionar que EE.UU. descansa esencialmente sobre el impulso de los particulares en materia de protección de datos, al igual que Chile; pero, a diferencia de nuestro país, el derecho norteamericano contempla la posibilidad de imposición de indemnizaciones no sólo compensato-

[64] Véase la crítica sobre este punto *supra* nota 14.

[65] Salvo, claro está, que uno considere como una ventaja el ahorro fiscal al evitar crear nueva institucionalidad. Pero incluso en esta perspectiva de mero cálculo financiero, desvinculada de consideraciones de protección de derechos, no resulta claro el "ahorro", dado el importante aumento de personal y recursos que el Sernac requeriría para hacer frente a las exigencias que la Ley Nº 19.628 reformada traería. Y ello, tan sólo para contar con una institucionalidad que no cumpliría realmente con sus objetivos, según damos cuenta en este trabajo.

rias, sino también punitivas y abdicativas[66], cuyos ingentes montos, que exceden con largueza la valorización del daño causado, obran el efecto de disciplinar a los agentes públicos y privados.

Vale decir, nuestro Proyecto de Reforma se queda "con lo peor de los dos mundos": impulso procesal, costos y mecanismos de cargo de los individuos afectados, pero sin incentivos adecuados a los privados para el cumplimiento (i.e. persecución por los titulares, respeto a la ley por los tratantes de datos). Todo ello debiera llevarnos a reevaluar los términos en que el Proyecto de Reforma está planteado, para tomarnos en serio la protección de los derechos fundamentales en general, y de la autodeterminación informativa en particular.

Precisamente por ser una cuestión obvia, creemos que vale la pena recordarlo, lo expuesto no quiere significar que propongamos importar una copia calcada de la AEPD y su institucionalidad a Chile. De hecho, la finalidad de protección de los datos personales y del derecho a la autodeterminación informativa puede lograrse de distintas maneras. Tal y como nos recuerda Rajevic, el derecho comparado proporciona una variedad de modelos, desde los que promueven una sola entidad a cargo del derecho de acceso a la información y de la protección de datos personales, como es el caso de la *Information Commissioner's Office* (ICO) en el Reino Unido[67]; hasta los que establecen dos órganos perfectamente diferenciados para cada ámbito, como ocurre en Canadá y Francia[68]. España, que establece un robusto sistema de protección de datos personales, carece, por contrapartida, de

[66] Sobre estos tipos de indemnización, véase Cane, Peter (1997). *The Anatomy of Tort Law.* Oxford, Hart Publishing, pp. 112-115. Una indemnización punitiva opera como multa civil, y su función es el castigo, no correspondiendo su monto a ningún daño o perjuicio experimentado por la víctima (los que fueron compensados vía indemnización *compensatoria*); y una indemnización abdicativa es, asimismo, un castigo para el agente del daño, a quien se le obliga a renunciar o "abdicar" *a favor de la víctima* de las ganancias obtenidas lícitamente a partir del daño ilícito causado a la misma, pero dichas ganancias *no se corresponden ni dicen relación con ninguna pérdida o detrimento* que haya experimentado la víctima.

[67] La *Freedom of Information Act* 2000 creó la ICO, encomendándole tanto las materias pertinentes al acceso a información pública, como a la protección de datos personales bajo la *Data Protection Act* de 1998. Se le confiere el poder para recibir reclamos, investigarlos y emitir decisiones sobre la materia, siendo sus decisiones apelables ante un tribunal de derechos de la información, el *Information Rights Tribunal*. Incluso la exposición somera de los principios generales y la regulación sobre la cual se articula un verdadero Derecho de la Información en el Reino Unido, excede con creces el ámbito y propósito de este trabajo, centrado en la legislación española. Bástenos aquí enunciar los principales cuerpos normativos que articulan el complejo sistema de información y privacidad a nivel nacional en el Reino Unido: *Freedom of Information Act* 2000 *(FOIA); The Environmental Information Regulations* 2004 *(EIR); INSPIRE Regulations* 2009 *(INSPIRE); Data Protection Act* 1998 *(DPA); Privacy and Electronic Communications Regulation* 2003 *(PECR); Data Protection Monetary Penalty Regulations* 2010 *(DP Monetarypenalties)*. Para una guía general sobre la *Information Commissioner's Office*, puede consultarse su sitio oficial: <http://www.ico.gov.uk/>.
Para un panorama (aunque no actualizado) del estado de la legislación sobre información alrededor del mundo, véase: Banisar, David (2002). *Freedom of Information and Access to Government Records Around the World.* Privacy, International. Disponible en: <http://www.forum.mn/res_mat/Freedom%20of%20Information%20records%20around%20world.pdf> [Consulta: 13 noviembre 2011].
Para una visión comprensiva de la legislación sobre protección de datos en el Reino Unido, véase: Carey, Peter (2009). *Data Protection: A Practical Guide to UK and EU Law*. Oxford University Press, 3ª Edición.

[68] Rajevic Mosler (2011), p. 156.

legislación integral e institucionalidad específica sobre acceso a la información pública[69], en lo que constituye una curiosa excepción a la tendencia occidental hacia el fortalecimiento de la transparencia.

Ya sea que se opte por un modelo unitario de protección informativa, o por entes diferenciados, sus particulares configuraciones pueden también variar en función de sus potestades sancionatorias y facultades de investigación y persecución. En Suecia[70], por ejemplo, la autoridad de control no cuenta con potestades para imponer sanciones por sí misma, al contrario de lo que sucede con el caso español, según vimos. Pero, como contrapartida a dicha configuración institucional, a la autoridad sueca se le confieren potestades procesales amplias para participar de procedimientos sancionatorios, perseguir y obtener la aplicación de sanciones ante tribunales por infracciones a las normas suecas sobre protección de datos.

Dicho de otro modo, lo relevante es que, cualquiera sea la particular configuración que escojamos, debe existir conciencia de que se trata de un bien jurídico cuya significancia y especiales características exceden del ámbito de lo meramente privado; y nuestras reglas institucionales, a la par con nuestros entendimientos sociales, debieran reflejar esa complejidad. Y cualquiera sea la configuración institucional por la que en definitiva se opte, un mismo elemento resulta central a todas ellas: la efectiva independencia de la autoridad de control de datos frente a los poderes del Estado.

Las consideraciones que he desarrollado en este trabajo me inclinan a preferir una agencia única, autónoma, cuya característica central debe ser su independencia con respecto a la Administración, en la cual se deposite la misión de protección de datos personales de manera exclusiva, siguiendo el modelo español en la materia, con las debidas adaptaciones, que comprenda las funciones de difusión y asistencia, registro, regulación, inspección y tutela cautelar en relación con la normativa sobre datos personales; ello, sin perjuicio de la existencia de mecanismos jurisdiccionales de tutela cautelar y reparación pecuniaria concurrentes. Si se opta por no entregarle potestades sancionatorias oficiosas, debería optarse, a lo menos, por entregarle potestades procesales amplias para perseguir responsabilidades por sí misma, sin que la sanción dependa del impulso privado. Tal institucionalidad contribuiría de manera más efectiva, a mi juicio, con una política pública coherente con un Estado democrático de derecho respetuoso de los derechos de las personas y activo promotor de la vigencia de tales derechos, además de sentar las bases para una transferencia de datos y conocimiento más segura y competitiva a nivel internacional.

[69] De particular interés resulta al respecto el trabajo de GUICHOT REINA, Emilio (2011). *Transparencia y Acceso a la Información Pública en España: análisis y propuestas legislativas.* Fundación Alternativas. Disponible en: <http://www.falternativas.org/laboratorio/documentos/documentos-de-trabajo/transparencia-y-acceso-a-la-informacion-publica-en-espana-analisis-y-propuestas-legislativas> [Consulta: 13 noviembre 2011].

[70] *Personuppgiftslag, Ley de Datos Personales* (1998:204). Texto en inglés disponible en: <http://www.regeringen.se/content/1/c6/01/55/42/b451922d.pdf> [Consulta: 12 noviembre 2011].

Bibliografía Citada

Arrieta, Raúl (2009). "Chile y la Protección de Datos Personales". En: *Chile y la Protección de Datos Personales: ¿Están en Crisis Nuestros Derechos Fundamentales?* Expansiva, Santiago: Ediciones Universidad Diego Portales. Disponible en: <http://www.expansiva.cl/media/publicaciones/libros/pdf/7.pdf> [Consulta: 13 noviembre 2011].

Banisar, David (2002). *Freedom of Information and Access to Government Records Around the World.* Privacy, International. Disponible en: <http://www.forum.mn/res_mat/Freedom%20of%20Information%20records%20around%20world.pdf> [Consulta: 13 noviembre 2011].

Cane, Peter (1997). *The Anatomy of Tort Law.* Oxford, Hart Publishing.

Carey, Peter (2009). *Data Protection: A Practical Guide to UK and EU Law*. Oxford University Press, 3ª Edición.

Centro de Estudios de Justicia de las Américas (CEJA) (2011). *Estudio de análisis de trayectoria de las Causas Civiles en los Tribunales Civiles de Santiago*. Informe Final, Santiago, mayo.

Cerda Silva, Alberto (2003). "Autodeterminación Informativa y Leyes sobre Protección de Datos". *Revista Chilena de Derecho Informático*, Santiago, Nº 3.

Cerda Silva, Alberto (2005). *La Autoridad de Control sobre Protección de Datos Personales.* Universidad de Chile, Anales de la Facultad de Derecho, Santiago, Nº 2.

Cerda Silva, Alberto (2006). "Mecanismos de Control en la Protección de Datos en Europa". *Ius et Praxis*, año 12, Nº 2.

Cerda Silva, Alberto (2011). "Enforcing Intellectual Property Rights by Diminishing Privacy: How the Anti-Counterfeiting Trade Agreement Jeopardizes the Right to Privacy". En: *Washington, American University International Law Review*, Washington College of Law, Vol. 26, Nº 3.

Fernando Magarzo, María del Rosario (2005). "La Protección de Datos Personales en el ámbito de la Publicidad en la Legislación Española". *Revista de Derecho Informático*, Nº 7.

Fundación ProAcceso (2011). *Estudio de Protección de Datos Personales en el Servicio Público*. Disponible en: <http://www.proacceso.cl/noticia/estudio_de_pro_acceso_revela_deficiencias_en_la_administraci_n_de_bases_de_datos_personales_> [Consulta: 2 octubre 2011].

Guichot Reina, Emilio (2011). *Transparencia y Acceso a la Información Pública en España: análisis y propuestas legislativas.* Fundación Alternativas. Disponible en: <http://www.falternativas.org/laboratorio/documentos/documentos-de-trabajo/transparencia-y-acceso-a-la-informacion-publica-en-espana-analisis-y-propuestas-legislativas> [Consulta: 13 noviembre 2011].

JIJENA LEIVA, Renato (2001). "La Ley Chilena de Protección de Datos Personales. Una Visión Crítica desde el Punto de Vista de los Intereses Protegidos". En: *Tratamiento de Datos Personales y Protección de la Vida Privada*, WAHL SILVA, Jorge (Edit.), Cuadernos de Extensión Jurídica, Universidad de los Andes, Nº 5, Santiago.

LÓPEZ ROMÁN, Eduardo (2009). "Un Análisis de la Estructura Institucional de Protección de Datos en España". *Revista para el Análisis del Derecho (InDret)*, Barcelona, Nº 2, mayo. Disponible en: <http://www.indret.com/pdf/641_es.pdf> [Consulta: 17 septiembre 2011].

LUCAS MURILLO DE LA CUEVA, Pablo (1999). "La Construcción del Derecho a la Autodeterminación Informativa". *Revista de Estudios Políticos*, España, Nº 104, abril-junio.

MONTOYA MARTÍN, Encarnación (2008). *Consideraciones sobre las Actuaciones Previas y su Incidencia en el Procedimiento Administrativo Sancionador y en las Garantías del Administrado*. Disponible en: <http://89.248.100.178/da/upload/280-9.pdf> [Consulta: 25 septiembre 2011].

PIÑAR MAÑAS, José Luis (2003). "La Agencia Española de Protección de Datos: Estructura y Funcionamiento". *Revista Chilena de Derecho Informático*, Nº 3, pp. 35 y ss.

PRIVACY INTERNATIONAL (2007). *The 2007 International Privacy Ranking.* Disponible en: <https://www.privacyinternational.org/article/leading-surveillance-societies-eu-and-world-2007#overview> [Consulta: 30 septiembre 2011].

RAJEVIC MOSLER, Enrique (2011). "Protección de datos y transparencia en la administración pública chilena: Inevitable y deseable ponderación". En: *Reflexiones sobre el Uso y Abuso de los Datos Personales en Chile*, Expansiva, Santiago. Disponible en: <http://www.redrta.org/Proteccin%20de%20Datos/Chile-Protecci%C3%B3n%20de%20datos%20y%20transparencia%20en%20la%20administraci%C3%B3n%20chilena.pdf> [Consulta: 13 noviembre 2011].

TAPIA RODRÍGUEZ, Mauricio (2008). "Fronteras de la vida privada en Chile". *Revista Chilena de Derecho Privado*, Fundación Fernando Fueyo, Nº 11. Disponible en: <http://www.fundacionfueyo.cl/revista/11_Revista_Fundacion_Fueyo.pdf> [Consulta: 30 septiembre 2011].

NORMAS CITADAS

A. Nacionales

Constitución Política de la República.

Código de Procedimiento Civil.

Ley Nº 19.223, que sanciona ilícitos penales relativos a la informática, *Diario Oficial*, 7 de junio de 1993.

Ley Nº 19.628, sobre protección de datos personales, *Diario Oficial*, 28 de agosto de 1999.
Ley Nº 19.880, sobre bases de los procedimientos administrativos, *Diario Oficial*, 29 de mayo de 2003.
Ley Nº 20.285, sobre acceso a la información pública, *Diario Oficial,* 20 de agosto de 2008.

B. Extranjeras

España:

Constitución Española, 1978.
Convenio 108 de 1981 adoptado por la Comunidad Europea.
Ley Nº 30/1992, 26 de noviembre.
Ley Nº 29/1998, 13 de julio.
Ley Orgánica 15/1999, 13 de diciembre.
Ley Nº 34/2002, 11 de julio.
Ley Nº 32/2003, 3 de noviembre.
Real Decreto 428/1993, 26 de marzo.
Real Decreto 156/1996, 2 de febrero.
Real Decreto 1720/2007, 21 de diciembre.
Real Decreto 1665/2008, 17 de octubre.

Suecia:

Personuppgiftslag (Ley de Datos Personales) 1998:204.

Reino Unido:

Freedom of Information Act, 2000.