ISSN 0717-9987

en foco 162

Protección de datos y transparencia en la administración pública chilena: Inevitable y deseable ponderación

Enrique Rajevic Mosler

* Ponencia presentada en el taller "Chile y la Protección de Datos Personales", organizado por Expansiva (Santiago, 26 de noviembre de 2010). Agradezco las observaciones realizadas por los asistentes a dicho encuentro y las formuladas a la primera versión de este texto por la profesora de la U. de Chile Andrea Ruiz R., aunque asumo mi responsabilidad personal por el resultado final y las opiniones aquí vertidas (erajevic@uahurtado.cl).

expansiva

I. Introducción

Con casi una década de diferencia los legisladores chilenos aprobaron la Ley 19.628, de 1999,[1] para regular la protección de datos personales (en adelante, LPDP), y la Ley 20.285, de 2008,[2] para normar el régimen del acceso a la información pública. Ambos cuerpos legales regulan el mismo objeto: la información. El primero cautela la información que concierne a personas naturales identificadas o identificables, desde una perspectiva que pretende garantizar que sus titulares sean quienes decidan sobre su uso. El ámbito del segundo, en cambio, es la información que obra en poder de los órganos del Estado (básicamente la administración pública) —la que puede incluir datos personales— con la óptica de favorecer su conocimiento por parte de la ciudadanía. La protección de los datos personales resguarda la intimidad y la autodeterminación informativa; la transparencia administrativa favorece la probidad y potencia la participación ciudadana. Todos ellos son bienes jurídicos reconocidos por nuestra Constitución y, potencialmente, antagónicos.

En efecto, parte de la información que obra en poder de los órganos públicos está constituida por datos personales. Ejemplos sobran, como los de los alumnos que estudian en colegios públicos, los jubilados en el sistema público de pensiones, los pacientes atendidos en hospitales públicos, los propios funcionarios o los beneficiarios de las múltiples prestaciones que otorga la administración estatal. El 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? No se trata de preguntas que sólo se generen entre nosotros, sino que de cuestionamientos que están presentes en todos los

El 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?

(1) Publicada en el D.O. de 28/08/1999.

(2) Publicada en el D.O. de 20/08/2008.

sistemas jurídicos que han llegado a regular estas instituciones.[3] Sin embargo, cada país debe construir una solución a la medida de las convicciones de sus ciudadanos y de su desarrollo institucional.

De este modo en las páginas que siguen abordaré cómo estamos afrontando este reto en Chile. Para ello describiré sucintamente los principios básicos de las normativas chilenas sobre protección de datos personales y acceso a la información pública, así como su anclaje constitucional; centrándome en esta última en la Ley de Transparencia (en adelante LT) contenida en el artículo primero de la Ley 20.285. A continuación me referiré a algunas fricciones entre ambas normativas y relataré cómo las ha ido resolviendo el organismo encargado de dirimir las contiendas sobre acceso a la información de la administración del Estado, el denominado "Consejo para la Transparencia" (en adelante CPT). Terminaré con algunas conclusiones y propuestas.

II. La protección de datos personales: Fundamentos y situación en el sector público

La LPDP define datos personales como aquellos relativos a cualquier información concerniente a personas naturales, identificadas o identificables (art. 2º f), a diferencia de los datos estadísticos que son aquellos que, en su origen, o como consecuencia de su tratamiento, no pueden ser asociados a un titular identificado o identificable (art. 2º e). Dentro de los datos personales existe una categoría que recibe mayor protección: los datos sensibles, que son los referidos "…a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida

La LPDP define datos personales como aquellos relativos a cualquier información concerniente a personas naturales, identificadas o identificables.

(3) A modo de ejemplo puede verse sobre el caso español a José L. Piñar M., *Seguridad, transparencia y protección de datos: El futuro de un necesario e incierto equilibrio*, Documento de Trabajo 147/2009, Madrid: Laboratorio de Alternativas. 2009, 64 p., y sobre el caso uruguayo a Carlos E. Delpiazzo, "A la búsqueda del equilibrio entre privacidad y acceso", en Carlos E. Delpiazzo (coord.) *Protección de datos y acceso a la información pública*, Agesic-FCU, Montevideo, 2008, p. 9-22.

sexual" (art. 2º. g). La misma definición se encuentra en la LT con un ligero matiz: "origen social" en vez de "racial" (art. 7º i, inc. 2º).

Nuestra ley no es sino el eco de las leyes de protección de datos que aparecieron en el último medio siglo de la mano del creciente desarrollo de la informática, el que ha permitido procesar datos de una manera que antes era completamente inconcebible y que desde el advenimiento de Internet permite transferirlos con enorme facilidad, todo lo cual pone en evidente riesgo la intimidad de las personas. Precisamente la LPDP parte anunciando que regula el "tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares" (art. 1º). Dos términos son aquí esenciales:

Nuestra ley no es sino el eco de las leyes de protección de datos que aparecieron en el último medio siglo de la mano del creciente desarrollo de la informática, el que ha permitido procesar datos de una manera que antes era completamente inconcebible y que desde el advenimiento de Internet permite transferirlos con enorme facilidad.

- Banco de datos, que es el "conjunto organizado de datos personales, sea automatizado o no y cualquiera sea la forma o modalidad de su creación u organización, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos" (art. 2 m). En consecuencia, no es cualquier dato suelto sino aquél que forma parte de un conjunto organizado que permita relacionamientos.

- Tratamiento, en tanto, es "cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma pública" (art. 2 o). La cantidad de verbos da cuenta de la amplitud de esta noción. Prácticamente toda utilización de un dato cabe dentro del concepto.

En el entorno comparado los orígenes de estas regulaciones pueden situarse en una ley estadounidense de 1974, la llamada "Privacy Act". En Europa, algunas constituciones en esa misma década afrontaron este tema —como el art. 18.4 de la Constitución española de 1978 o el art. 35 de la Constitución Portuguesa de

1976— y en 1981 el Consejo de Europa aprobó el Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Se trata de textos que influirán en todas las normas posteriores.(4) A nivel internacional se destaca luego la Directiva 95/46/CE del Parlamento y del Consejo Europeo 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,(5) que en tal carácter será el molde de las legislaciones de sus países miembros (en el caso español, por ejemplo, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal).(6) A su vez, el art. 8º de la Carta de Derechos Fundamentales de la Unión Europea (2000) reconoce a toda persona el "…derecho a la protección de los datos de carácter personal que le conciernan", añadiendo que aquéllos "se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley". Termina indicando que "toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación".

(...) no se trata del puro derecho a ser dejado solo, en la formulación decimonónica del derecho a la intimidad* (the right to be let alone)*, sino del derecho a la autodeterminación informativa, esto es, el derecho de las personas a controlar sus datos personales, incluso si éstos no se refieren a su intimidad.

La protección de los datos personales es una derivación del derecho a la intimidad que, según la doctrina, llega a configurar un nuevo y específico derecho fundamental de tercera generación,(7) reconocido ya en 1983 en la sentencia del tribunal constitucional alemán en el caso de la Ley de Censo de Población. En efecto, no se trata del puro derecho a ser dejado solo, en la formulación decimonónica del derecho a la intimidad (*the right to be let alone*), sino del

(4) A modo de ejemplo la definición de datos personales en el Convenio 108 es "cualquier información relativa a una persona física identificada o identificable" (art. 2º a) y, aunque no habla de datos sensibles, declara que: "Los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas. La misma norma regirá en el caso de datos de carácter personal referentes a condenas penales" (art. 6º).

(5) DOCE L 281, de 23/11/1995.

(6) BOE núm. 298, de 14/12/1999.

(7) Véase la sentencia del Tribunal Constitucional español 292/2000, del 30 de noviembre, esp. su FJ 7, y sobre esta generación de derechos Antonio Pérez L., La Tercera Generación de Derechos Humanos, Navarra: Aranzadi, 2006, 320 p.

derecho a la autodeterminación informativa, esto es, el derecho de las personas a controlar sus datos personales, incluso si éstos no se refieren a su intimidad.(8) En otras palabras, no sólo se trata de una noción negativa o abstencionista (excluir a otros) sino también una positiva (controlar mis datos). Con todo, la protección no se opone a reconocer que la circulación de estos datos también es una necesidad social. Se trata, en definitiva, de aprovechar los beneficios que brindan a la sociedad las nuevas tecnologías informáticas de una manera que respeten los derechos de las personas.

En Chile el derecho a la intimidad se encuentra reconocido en el artículo 19 Nº 4 de la Constitución que asegura el "respeto y protección a la vida privada y a la honra de la persona y su familia".

En Chile el derecho a la intimidad se encuentra reconocido en el artículo 19 Nº 4 de la Constitución que asegura el "respeto y protección a la vida privada y a la honra de la persona y su familia". De hecho, la Ley 19.628 aparece titulada como "ley sobre protección de la vida privada" además de "ley sobre protección de datos de carácter personal". Con todo, tras este frontis "protector" lo primero que hace es reconocer que toda persona puede tratar datos personales si se ajusta a sus normas. La doctrina ha puesto de relieve sus insuficiencias, como la ausencia de un órgano efectivo de fiscalización, un *habeas data* judicial poco operativo (de hecho, apenas utilizado) y un talante tolerante con los tratamientos que realizan algunos agentes privados en materia comercial.(9) Esto hace que no cumplamos integralmente ni con las directrices de la OCDE(10) ni con los estándares de la Directiva 95/46/CE para que la UE nos declarase un país seguro para el flujo de datos desde sus estados miembros (cosa que ya han logrado Argentina en 2006 y Uruguay en 2010).

Pese a la necesidad de los apuntados perfeccionamientos, los preceptos de la LPDP establecen un sistema que ha venido a ordenar el tratamiento de datos

(8) Véase sobre esto Isabel-Cecilia del Castillo V. *Protección de datos: Cuestiones constitucionales y administrativas.* Madrid: Thomson-Civitas, 2007, p. 213-241.

(9) Puede verse a este respecto Renato Jijena L. *Comercio Electrónico, Firma Digital y Derecho*. Santiago, Editorial Jurídica, 2002. p. 75-78. También puede consultarse Pedro Anguita R. *La Protección de datos personales y el derecho a la vida privada*. Santiago, Editorial Jurídica, 2007. p. 331-342, y Raúl Arrieta C., "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?*, Expansiva UDP, Santiago de Chile, 2009, p. 18-21.

(10) Me refiero a las "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", de 23/09/1980. Pueden verse en español en el sitio de la Agencia Española de Protección de Datos (http://www.agpd.es).

personales evitando al menos algunos abusos. Lo primero que merece consignarse es que puede derivarse una serie de principios para el tratamiento, todos los cuales se aplican a la administración pública. Se trata de los siguientes:

a) El principio de licitud que deriva de los artículos 2º, 4º incisos 1º y 6º, y según el cual el tratamiento sólo cabe si existe autorización legal o de parte del titular, debiendo en este último caso tratarse de un consentimiento expreso.

b) El principio de información al titular respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público, establecido en el art. 4°, inc. 2º.

c) El principio de veracidad de los datos, que exige corregir los que sean erróneos, inexactos, equívocos o incompletos (art. 6°, inc. 2°).

d) El principio de finalidad de los datos, que fluye del art. 9º, y conforme al cual debe respetarse la finalidad para la que fueron recogidos los datos, de manera que exista una relación directa entre aquella y el dato recabado.

e) El principio de seguridad de los datos, contemplado y cautelado en el art. 11 y, tratándose de los órganos de la Administración, por el D.S. N° 83/2004, SEGPRES.

f) El principio de confidencialidad que se aplica cuando se trata de datos obtenidos de fuentes no accesibles al público según el art. 7º.

Por otro lado, la ley reconoce un conjunto de derechos a los titulares de datos personales. Se trata de los derechos de acceso, rectificación, cancelación y bloqueo. El primero permite a toda persona exigir al responsable de un banco información sobre qué datos de su titularidad está tratando y, además, sobre "…su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente" (art. 12, inc. 1º). El derecho a rectificar permite exigirle que modifique los datos "erróneos, inexactos, equívocos o incompletos" (art. 12, inc. 2º) y el de cancelación, que los elimine "en caso de que su almacenamien-

to carezca de fundamento legal o cuando estuvieren caducos" (art. 12, inc. 3º) o cuando cese el consentimiento para su uso, si fueron obtenidos voluntariamente o se usan para comunicaciones comerciales (art. 12, inc. 4º). En esta última hipótesis también cabe el derecho de bloqueo, esto es, a exigir la suspensión temporal de cualquier operación de tratamiento. Debe señalarse que no existe un derecho de oposición al tratamiento, en los términos que existen en el derecho comparado.

El ejercicio de estos derechos es irrenunciable (art. 13), pero no cabe respecto de los órganos públicos cuando "impida o entorpezca el debido cumplimiento de las funciones fiscalizadoras del organismo público requerido, o afecte la reserva o secreto establecidos en disposiciones legales o reglamentarias, la seguridad de la Nación o el interés nacional" o, si el almacenamiento fue por mandato legal, "fuera de los casos contemplados en la ley respectiva" (art. 15).[11]

El art. 16 de la LPDP garantiza el ejercicio de estos derechos a través de una acción que debe interponerse ante el juez de letras en lo civil del domicilio del responsable del banco de datos o ante la Corte Suprema, si la causal invocada para denegar la solicitud fuese la seguridad de la nación o el interés nacional. De acogerse la reclamación puede aplicarse una multa de hasta 50 unidades tributarias mensuales. Hay, asimismo, derecho a ser indemnizado por el daño patrimonial y moral que causare el tratamiento indebido de los datos en los términos del art. 23 de la LPDP.

(...) la ley proscribe el tratamiento de los datos sensibles salvo que la ley lo autorice, exista consentimiento del titular o se trate de datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares (...)

Finalmente, debe destacarse que la ley proscribe el tratamiento de los datos sensibles salvo que la ley lo autorice, exista consentimiento del titular o se trate de datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares (art. 10).

El título V de la LPDP, de apenas tres artículos, regula el tratamiento de datos por parte de los organismos públicos. Cabe recordar que el art. 1º aplica a éstos ultimos las normas generales, de manera que este título contiene sólo especificaciones para los organismos públicos.

(11) El inciso 2º del art. 15 es una norma oscura, pues los órganos de la Administración no debiesen almacenar datos sin mandato legal, pero no hay espacio para ahondar en ello.

El artículo 20 refuerza el principio general de licitud al restringir el tratamiento de datos a las materias que sean de competencia de cada organismo y "con sujeción a las reglas precedentes". En esas condiciones, añade, la administración "no necesitará el consentimiento del titular". Esto constituye, en mi opinión, una autorización que abre el tratamiento de datos personales con relativa amplitud —incluso en el ámbito de las potestades domésticas de la Administración— pero con el resguardo de aplicar a este tratamiento las demás reglas de la ley que salvaguardan los derechos de los particulares. Para ello tiene especial interés la regla de la finalidad establecida en el art. 9º, que al restringir el uso de los datos a los fines para los cuales fueron recolectados proscribe su entrega a terceros para otras finalidades, en lo que no es sino una aplicación estricta del sistema de vinculación positiva del principio de juridicidad.(12)

El art. 21, por su parte, impide a los organismos que sometan a tratamiento "datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias" que los comuniquen "una vez prescrita la acción penal o administrativa, o cumplida o prescrita la sanción o la pena". Se trata de una especie de "derecho al olvido" que favorece la reinserción de las personas, especialmente tratándose de condenas penales. Se exceptúan de lo anterior las solicitudes formuladas por los tribunales u otros organismos públicos dentro del ámbito de su competencia (art. 21, inc. 2º).

Finalmente, el art. 22 encarga al Servicio de Registro Civil e Identificación llevar un registro de los bancos de datos personales a cargo de organismos públicos, el que fue reglamentado por el D.S. N° 779/2000, del Ministerio de Justicia.(13) No hay, sin embargo, sanciones para el incumplimiento de este deber.

III. El acceso a la información pública como derecho

El derecho de acceso a la información pública fue reconocido en Chile por la Ley 19.653, de 1999, sobre Probidad Administrativa, que consagró como regla general la publicidad de los actos administrativos y la de "los documentos que les sirvan de sustento o complemento directo y esencial", restringiendo la

(12) Art. 2º de la Ley 18.575, de 1986, cuyo texto refundido, coordinado y sistematizado fue fijado por el D.F.L. N° 1/19.653 (D.O. 17.11.2001).

(13) Disponible en http://www.srcei.cl/f_banco_de_datos.html.

reserva a un listado basado en cuatro causales que podía ser desarrollado por vía reglamentaria y admitiendo una impugnación en sede judicial. Es interesante destacar que esta última era semejante a la del art. 16 de la LPDP, incluso con la diferenciación de un procedimiento ante el juez en lo civil y otro ante la Corte Suprema, este último cuando se alegase la afectación de la seguridad de la nación o el interés nacional (art. 14).

Pues bien, en tan sólo una década diversos factores llevaron a un cambio radical. Entre éstos conviene destacar la sentencia de la Corte Interamericana de Derechos Humanos en el caso "Claude Reyes y otros vs. Chile",(14) que declaró que el sistema de acceso a la información chileno infringía el art. 13 de la Convención Americana sobre Derechos Humanos o Pacto de San José, pues éste garantizaba "el derecho que tiene toda persona a solicitar el acceso a la información bajo el control del Estado" (párrafo 77). Ello venía a significar que este derecho se integraba a nuestra Carta Fundamental en virtud de su art. 5°, que exige a los órganos del Estado respetar y promover los derechos esenciales que emanan de la naturaleza humana garantizados "por los tratados internacionales ratificados por Chile y que se encuentren vigentes", uno de los cuales es el Pacto de San José. El propio Tribunal Constitucional declaró que el acceso a la información administrativa estaba implícitamente reconocido por la Constitución, pues el art. 19 Nº 12 de la Constitución además de contemplar la "libertad de emitir opinión e informar" abarcaba el derecho a buscar y recibir información.(15) Además, desde la reforma constitucional de 2005(16) la transparencia pasó a constituir una de las Bases de la Institucionalidad pública chilena, al incorporarse un nuevo artículo 8º a nuestra Carta Fundamental, cuyo inciso 2º dispone que: "Son públicos los actos y resoluciones de los órganos del Estado, así como sus fundamentos y los procedimientos que utilicen. Sin embargo, sólo una ley de quórum calificado podrá establecer la reserva o secreto de aquéllos o de éstos, cuando la publicidad afectare el debido cumplimiento de

(...) en tan sólo una década diversos factores llevaron a un cambio radical. Entre éstos conviene destacar la sentencia de la Corte Interamericana de Derechos Humanos.

(14) Serie C 151, de 19 de septiembre de 2006.

(15) Sentencia del Tribunal Constitucional Rol Nº 634/2006, de 9 de agosto de 2007, considerando 9º.

(16) Ley de Reforma Constitucional Nº 20.050 (D.O. 26.08.2005).

las funciones de dichos órganos, los derechos de las personas, la seguridad de la Nación o el interés nacional".

Sobre esta base se dictó la LT, que establece el deber de los órganos públicos de publicar en Internet información relevante sobre su gestión (la llamada "Transparencia Activa") y de entregar la demás información que le sea requerida y obre en su poder, salvo que concurran los casos de reserva que detalla en sus artículos 21 y 22. Con todo, la innovación principal es la creación del "Consejo para la Transparencia" (en adelante CPT), organismo encargado de fiscalizar el cumplimiento de las normas sobre transparencia activa y resolver los reclamos en contra de las negativas a las solicitudes de acceso a la información, además de velar porque la administración pública cumpla con la LPDP. Su configuración favorece fuertemente su autonomía efectiva: es una "corporación autónoma de derecho público" (art. 31) que propone al Presidente sus propios "estatutos" (art. 41), cuya dirección y administración superior corresponde a un consejo directivo integrado por 4 consejeros, designados por el Presidente de la República "previo acuerdo del Senado, adoptado por los dos tercios de sus miembros en ejercicio" (art. 36) y que gozan de inamovilidad relativa (art. 38). Todo ello transforma al CPT en una verdadera "administración independiente",[17] facultada para sancionar a subsecretarios y jefes de servicio en general (arts. 45 a 49). El procedimiento de acceso, en tanto, es relativamente ágil y contempla una reclamación de ilegalidad ante la Corte de Apelaciones (arts. 28 y ss.).

(...) la innovación principal es la creación del "Consejo para la Transparencia" (en adelante CPT), organismo encargado de fiscalizar el cumplimiento de las normas sobre transparencia activa y resolver los reclamos en contra de las negativas a las solicitudes de acceso a la información.

Desde la vigencia de la LT, el 20 de abril de 2009, y hasta finalizado el 2010, el CPT ha resuelto cerca de 1.600 casos.[18] Esto que marca un fuerte contraste con el escaso puñado de sentencias judiciales que resolvieron reclamaciones de esta índole en los 10 años de vigencia del sistema de la Ley 19.653.

(17) Véase Enrique Rajevic M., "El Consejo para la Transparencia como «Administración Independiente»", en Raúl Letelier W. y Enrique Rajevic M. (coords.) *Transparencia en la Administración Pública*, Abeledo Perrot, Santiago de Chile, 2010, p. 241-8.

(18) Sobre esto puede verse Enrique Rajevic M., "El primer año de la jurisprudencia del Consejo para la Transparencia". /en/ VV.AA. *Transparencia en el Ámbito Público y Privado. Balance y Desafíos Pendientes.* Santiago de Chile, Chile Transparente, p. 55-71.

IV. La intersección entre la transparencia y la protección de datos personales: Algunos ejemplos y criterios de solución en la jurisprudencia del Consejo para la Transparencia

Definido sucintamente el ámbito de la protección de datos personales y de la transparencia administrativa conviene recordar que ya el artículo 8º de la Constitución reconoce como uno de los límites de la difusión de la información de los órganos del Estado la afectación de los derechos de las personas. La LT señala que entre estos derechos se encuentran los relativos a la seguridad de las personas, su salud, la esfera de su vida privada o derechos de carácter comercial o económico (art. 21 Nº 2). La referencia a la vida privada abre de inmediato campo a la LPDP. Ello es particularmente importante porque el art. 5º de la LT declara que toda la información que obre en poder de los órganos de la administración es pública, mientras su artículo 11, letra a, presume relevante toda información que éstos posean, cualquiera sea su origen o procesamiento. En consecuencia, la carga de la prueba de la reserva le corresponde al titular del derecho afectado que, además, debe ser atribuido por el ordenamiento "…en título de derecho y no de simple interés", conforme el art. 7º Nº 2 del reglamento de la ley.(19)

Para ello el art. 20 establece que los terceros que pudieren ver afectados sus derechos producto de una solicitud de información tienen derecho a ser notificados de ella y a oponerse dentro de tres días, lo que impide su entrega y exige del requirente acudir al CPT si es que desea persistir en la solicitud. Esta parece ser la forma en que debiera operar la causal de reserva del art. 21 Nº 2. Sin embargo, esto no es absoluto. El artículo 21 Nº 5 de la LT establece también el secreto de los "documentos, datos o informaciones que una ley de quórum calificado haya declarado reservados o secretos, de acuerdo a las causales señaladas en el artículo 8º de la Constitución Política", y su art. 1º transitorio entiende que cumplen con este quórum calificado los preceptos legales vigentes que establecen casos

(...) los terceros que pudieren ver afectados sus derechos producto de una solicitud de información tienen derecho a ser notificados de ella y a oponerse dentro de tres días, lo que impide su entrega y exige del requirente acudir al CPT si es que desea persistir en la solicitud.

(19) Aprobado por el D.S. N° 13/2009, del Ministerio Secretaría General de la Presidencia (D.O. 13.04.2009).

de secreto y son anteriores a la reforma constitucional de 2005 —que exigió ese quórum reforzado— con tal que se ajusten a las causales que señala el artículo 8º de la Constitución Política. En esas condiciones, la reserva que establece el artículo 7º de la LPDP —fundada en los derechos de las personas, como admite la Constitución— es válida y puede ser aplicada directamente.

En materia de transparencia activa la LT establece el deber de publicar en Internet las nóminas de beneficiarios de los programas sociales en ejecución, pero añade que no se incluirán en estos antecedentes los datos sensibles (art. 7º, letra i), criterio que el Consejo extendió a la publicación de actos y resoluciones que tengan efectos sobre terceros en su Instrucción General Nº 4, sobre transparencia activa aplicando directamente la LPDP.[20]

Finalmente, el artículo 33, letra m, encarga al CPT "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". En esto se siguió la inspiración del *Information Commissioner*, del Reino Unido, que está encargado de fiscalizar el cumplimiento de las leyes de transparencia y protección de datos personales, pero sólo embrionariamente como se desprende del literal citado.

Cerca de la cuarta parte de las decisiones de fondo dictadas por el CPT durante el último trimestre tuvieron que ver con datos personales en mayor o menor medida, esto es, una de cada cuatro, lo que significa que en sede de acceso a la información es relativamente frecuente que deba aplicarse la LPDP.

Dicho esto conviene recordar las reflexiones iniciales de este trabajo que apuntaban a las inevitables tensiones entre el derecho de acceso a la información. La evidencia no hace sino confirmarlo. Cerca de la cuarta parte de las decisiones de fondo dictadas por el CPT durante el último trimestre tuvieron que ver con datos personales en mayor o menor medida, esto es, una de cada cuatro, lo que significa que en sede de acceso a la información es relativamente frecuente que deba aplicarse la LPDP. Algunos casos en los que esto ha ocurrido son los siguientes:[21]

(20) La oración final de su punto 1.7 ordena a los órganos administrativos "…abstenerse de publicar datos personales que tengan carácter reservado conforme a lo establecido en los artículos 7°, 10, 20 y siguientes de la Ley 19.628, de protección de datos de carácter personal" (D.O. 03.02.2010).

(21) Cito las decisiones del CPT según el rol del caso. Su texto puede consultarse en el sitio web del Consejo (http://www.consejotransparencia.cl/).

a) **Protección del Rol Único Tributario (o RUT) y del domicilio:** El RUT es un código numérico creado por el D.F.L. N° 3/1969, ministerio de Justicia (D.O. 15/02/1969), con el fin de identificar "…a todos los contribuyentes del país, de los diversos impuestos, y otras personas o entes que se señalan más adelante" (art. 1°, inc. 1°). En las decisiones A10-09 y A126-09, del 31 de julio de 2009, se rechazó entregar los RUTs de un grupo de funcionarios y ex funcionarios afirmando que éste constituía un dato personal «…cuyo tratamiento sólo puede efectuarse cuando dicha ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello (art. 4° LPDP). En tal carácter, quienes trabajen "en el tratamiento de datos personales, tanto en organismos públicos como privados, están obligadas a guardar secreto sobre los mismos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público" (art. 7° Ley 19.628), esto es, aquéllas de acceso no restringido o reservado a los solicitantes» (considerando 8º). Aplicando el art. 20 de la LPDP se afirmó que «el R.U.T. de los funcionarios es un dato personal obtenido de los propios interesados en acceder a la función pública (art. 13 del Estatuto Administrativo), y no directamente de un registro público, sólo para su tratamiento al interior del servicio público respectivo y no para su cesión a terceros, por lo que debiera ser secreto o reservado». Por otro lado, como el personal de los organismos públicos se informa a través de la nómina de sus nombres en los sitios webs de transparencia activa de cada servicio, como dispone el art. 7° d) de la Ley de Transparencia, la información solicitada se entregó asociándola a los nombres, como dato ya conocido (como también establece el art. 17, letra b, de la Ley 19.880), resolviéndose así la ponderación entre transparencia y protección de datos. Este razonamiento ha sido empleado también respecto del RUT de los particulares y a propósito de los domicilios particulares de los funcionarios (por ejemplo la decisión C446-09).

b) **Sanciones y multas cumplidas o prescritas o con acción prescrita**: En materia de sanciones disciplinarias el Consejo ha aplicado el derecho al olvido del art. 21 LPDP (por ejemplo, los casos C73-10 y C111-10), salvo cuando existe un elevado interés público en el conocimiento de esta información (como ocurrió en las decisiones de los casos C411-09 y

C664-10). Un ejemplo son los resultados de sumarios sanitarios, pues tras el ejercicio de ponderación el Consejo ha estimado que la transparencia debe prevalecer sobre la protección de los datos personales.

c) **Datos relativos a los procesos de calificación o al cumplimiento de jornada de los funcionarios públicos:** Si bien se trata de datos personales el CPT ha entendido que al ser información elaborada con fondos públicos es, en principio, de acceso público, conforme al art. 5º LT, lo que se confirma al no haber una verdadera afectación de derechos dado que "…los funcionarios públicos poseen una esfera de vida privada más delimitada en virtud precisamente de la función que ejercen" (decisión A47-09, considerando 12°). En el mismo sentido se ha dicho que si las remuneraciones de los funcionarios son públicas en virtud del art. 7º, letra d, de la LT, e incluso objeto de transparencia activa —publicación en Internet—, también deben ser públicos los registros de control de asistencia, añadiendo que han sido producidos en el ejercicio de una función pública y que su conocimiento es relevante para el adecuado control social de aquella, lo que refuerza el art. 30 de la Ley 19.733 o Ley de Prensa al calificar como hechos de interés público los referentes al desempeño de funciones públicas (decisiones de los amparos A181-09, C434-09, C485-09, C492-09, C209-10 y C846-10). En consecuencia, en este caso la ponderación se resuelve a favor de la transparencia.

d) **Datos personales relativos a concursos públicos de personal:** En materia de concursos la ponderación ha llevado a una serie de distinciones, prevaleciendo en algunos casos el derecho de acceso y en otros la protección de los datos, si bien en estricto rigor estos últimos son resguardados como una exigencia para el debido funcionamiento de los sistemas de concurso y no en virtud de la LPDP. Así, el Consejo admite la solicitud de puntajes propios y de terceros, siempre que la identidad de estos últimos sea previamente conocida (en caso contrario debe aplicarse el art. 20 LT), pero no ha aceptado entregar los informes psicolaborales ni tampoco las referencias dadas por terceros por entender que ello afectaría sustantivamente el debido funcionamiento de los sistemas de reclutamiento. Con todo, tratándose de los candidatos designados para

el cargo últimamente el Consejo ha aceptado entregar tales informes en los concursos de alta dirección pública, afirmando que en tales cargos hay un alto interés público que supone un estándar de escrutinio ante el que debe ceder la privacidad (como en el caso de la decisión A336-10). Cabe señalar que en lo relacionado con los concursos de la Alta Dirección Pública la Dirección Nacional del Servicio Civil ha defendido el secreto de los procesos y los candidatos, fundada en los artículos 50º y 55º de la Ley 19.882 y reclamando la ilegalidad de las decisiones del Consejo. A la fecha existen dos sentencias de la Corte de Apelaciones de Santiago, una acogiendo y otra rechazando.[22]

e) **Datos sensibles:** El CPT ha declarado la reserva de datos relativos a la salud de las personas (p. ej., decisiones A211-09 y C240-10) y su militancia política (A152-09). Acá, en consecuencia, no se ha ponderado acceso con protección sino que ha prevalecido directamente la protección de los datos.

f) **Padrón Electoral:** En su decisión C407-09 el Consejo validó la entrega del padrón electoral del Servicio Electoral debido a que la Ley 18.556, orgánica constitucional del Sistema Electoral, prescribe categóricamente que los registros electorales deben ser públicos y que en base a ellos el Servicio Electoral elabora su padrón computacional. Si bien esta ley se aplicó por sobre la LPDP[23] también según esta última podría entenderse que no era confidencial, en tanto información contenida en una fuente accesible al público (art. 7º LPDP).[24] También el Consejo valoró que el control social del padrón electoral permitiría verificar que no existan inscripciones duplicadas (lo que incluso justifica en este caso entregar el RUT). Aunque se llegó a este resultado el Consejo sopesó también la afectación de los datos personales y admitió explícitamente su preocupación por la difusión

(22) Se trata de las sentencias roles 943-2010, de 03/09/2010, y 2080-2010, de 22/11/2010, ambas de la cuarta sala y la última, recurrida de queja.

(23) La decisión da a entender que se trata de un tema de jerarquía normativa. En mi opinión se trataría de un problema de competencia de las normas, esto es, el acceso al padrón electoral sería una materia orgánica constitucional vedada a la regulación de la ley simple.

(24) Aunque en tal caso debiese haberse reservado la condición de invidencia, lo que no se hizo.

resultante, para terminar afirmando que ante la claridad de la Ley 18.556, "…corresponde a los órganos colegisladores y no a este Consejo resolver, a futuro, si es preciso modificar este estado de cosas".(25)

g) **Personas Jurídicas:** El Consejo ha desconocido la protección de datos personales relativos a personas jurídicas por aplicación de la LPDP, que las excluye (por ejemplo, decisiones A39-09 y A309-09), pero ha reservado datos relativos a éstas fundándose en otros derechos por aplicación del art. 21 Nº 2 LT (p. ej., decisión A265-09) en otro ejercicio de ponderación.

h) **Ejercicio del derecho de acceso a datos personales en poder de la Administración Pública a través de la LT:** Por último, y para cerrar esta breve recapitulación, el CPT ha admitido que los titulares de datos personales puedan requerirlos a través de los mecanismos de la LT y no sólo mediante el *habeas data* regulado por la LPDP, de manera que se trataría de mecanismos alternativos para obtener el mismo propósito. Así ha ocurrido con datos relativos a concursos, solicitud de indultos, procedimientos administrativos, etcétera (como las decisiones C178-10 y C426-10).

Creo que los casos anteriores son suficientemente ilustradores de la importancia que tiene la LPDP en la tarea que realiza el CPT. Probablemente se trata del organismo público que ha debido darle una aplicación más intensiva, al punto que esté estudiando la elaboración de una recomendación sobre esta materia. En los casos que hemos revisado el CPT valora los datos personales como una posible excepción a la transparencia administrativa, siguiendo la lógica del art. 8º de la Constitución y el art. 21 de la Ley de Transparencia. Existen otros ordenamientos que invierten la regla, de

Creo que los casos anteriores son suficientemente ilustradores de la importancia que tiene la LPDP en la tarea que realiza el CPT. Probablemente se trata del organismo público que ha debido darle una aplicación más intensiva, al punto que esté estudiando la elaboración de una recomendación sobre esta materia.

(25) Hay una disidencia del Consejero y entonces Presidente Juan Pablo Olmedo, quien aplicando el principio de finalidad postuló que el padrón computacional sólo podía entregarse suprimiendo la profesión, fecha de nacimiento, domicilio, RUT e indicación de la condición de no vidente o analfabeto de las personas inscritas.

manera que si la información solicitada a la Administración puede afectar la privacidad de una persona se entiende que es reservada, debiendo el solicitante acreditar la existencia de un interés público que justificase su revelación.(26)

No obstante, para evaluar la procedencia o improcedencia de las causales de reserva invocadas, el CPT ha aplicado numerosas veces un test de daño (decisión A45-09, del 28 de julio de 2009, considerandos 8º a 11º) y un test de interés público (decisión A115-09, del 22 de agosto de 2009, considerandos 11º y 12º): "Ambos, que pueden ser complementarios, consisten en realizar un balance entre el interés de retener la información y el interés de divulgarla para determinar si el beneficio público resultante de conocer la información solicitada es mayor que el daño que podría causar su revelación. El primero se centra en ponderar si la divulgación puede generar un daño presente, probable y específico a los intereses o valores protegidos de mayor entidad que los beneficios obtenidos; el segundo, en ponderar si el interés público a obtener con la entrega de la información justifica su divulgación y vence, con ello, la reserva" (decisión C193-10). Se trata de un ejercicio de ponderación de derechos, como se dijo en la decisión A45-09, que exige respetar el principio de proporcionalidad y el contenido esencial de uno y otro derecho.(27)

(26) Por ejemplo, la Privacy Act canadiense, en vigor desde el 1º de julio de 1983, parte del principio de la reserva de los datos personales y permite en su art. 8 que puedan comunicarse a terceros sin consentimiento del titular sólo en casos excepcionales, uno de los cuales es que, en opinión del jefe de la institución, *"(i) el interés público en la divulgación sea claramente mayor que el perjuicio a la privacidad que podría generarse, o (ii) la divulgación beneficie claramente a la persona a quien se refiere la información"* (art. 8.2.m). A este respecto se ha dicho que "…la discrecionalidad en el otorgamiento a la Administración de la potestad para otorgar o no el acceso a la información es aquí doble: la ley de protección de datos deja la decisión al juicio del responsable de la institución, y la Ley de Acceso, como dijimos, establece, en general, que en los casos de comunicaciones inconsentidas conforme al artículo 8 de la Ley de Protección de Datos [*Privacy Act*] el acceso puede (o no) acordarse. Se trata de un supuesto que requiere un aquilatado juicio ponderativo para el que la Administración goza de un importante margen de discrecionalidad". Emilio Guichot R. Publicidad y privacidad de la información administrativa. Madrid: Civitas, 2009, p. 36.

(27) Su considerando 10º señala que: ["...Establecido que estamos en presencia de un derecho de rango constitucional la reserva o secreto pasa a limitarlo o restringirlo, por lo que debe respetar el principio de proporcionalidad que supone analizar, conforme señala la doctrina: a) si la medida es eficaz, b) si no existe un medio más moderado para la consecución eficaz del propósito buscado (en este caso, cautelar el secreto) y, por último, c) si de la medida a adoptar (en este caso, el secreto absoluto) derivan más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (véase BERNAL P., Carlos. El principio de proporcionalidad y los derechos fundamentales, 2ª ed. Madrid: Centro de Estudios Políticos y Constitucionales, 2005, y GARCÍA P., Gonzalo y CONTRERAS V., Pablo. Derecho de Acceso a la Información en Chile: Nueva Regulación e Implicancias para el Sector de la Defensa Nacional. /en/ Estudios Constitucionales año 7, N° 1, 2009, p. 144)". En términos semejantes nuestro Tribunal Constitucional ha dicho sobre este principio lo siguiente: "Reiterando nuestra jurisprudencia constitucional anterior (Sentencia Rol N° 226, Considerando 47, y Sentencia Rol Nº 280, Considerando 29), una limitación a un derecho fundamental es justificable cuando dicho mecanismo es el estrictamente necesario o conveniente para lograr un objetivo constitucionalmente válido, debiendo consecuentemente el legislador elegir aquellas limitaciones que impliquen gravar en menor forma los derechos fundamentales" (Sentencia Rol N° 519/2006, de 5 de junio de 2007, consid. 19°)"].

V. Conclusiones

Del análisis realizado se desprende con claridad que la protección de datos personales y la transparencia son desarrollos de derechos fundamentales que se proyectan sobre un mismo objeto: la información que está a disposición de los organismos públicos. De allí que se haya dicho que sean dos caras de una misma moneda.

Del análisis realizado se desprende con claridad que la protección de datos personales y la transparencia son desarrollos de derechos fundamentales que se proyectan sobre un mismo objeto: la información que está a disposición de los organismos públicos.

Lo anterior exige que necesariamente deban armonizarse a través del mecanismo de la ponderación de derechos, para lo cual existen distintos enfoques y soluciones institucionales en el derecho comparado, desde las que promueven una sola entidad a cargo de ambos temas, como el Information Commissioner Office (ICO) en Reino Unido —que es el modelo que se propuso en el proyecto de ley discutido en la Cámara de Diputados[28]—, o el Instituto Federal de Acceso a la Información (IFAI) mexicano, hasta los que auspician la existencia de dos órganos perfectamente diferenciados, como ocurre en Canadá y Francia. En cualquier modelo es clave la autonomía e independencia de esta autoridad.[29] De seguir Chile la primera alternativa sería precisa una profunda reorganización del CPT (acompañada de los medios necesarios) y/o una reorientación en las capacidades de su personal, que le permitiera actuar eficazmente en el ámbito de la protección de datos en poder de agentes privados, ámbito que cuantitativamente es más significativo que el de los datos en poder del Estado.[30] Optar por la creación

(28) En el marco de la tramitación del proyecto de ley que introduce modificaciones a la Ley 19.628 y a la ley N° 20.285 (Boletín N° 6120-07), actualmente en primer trámite constitucional, que transforma al CPT en el "Consejo para la Transparencia y Protección de Datos Personales".

(29) 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 (DOUE L 281, de 23.11.1995), exige en su art. 28 Nº 1 que las autoridades encargadas de controlar la aplicación de las disposiciones sobre protección de datos personales ejerzan las funciones que les son atribuidas "…con total independencia", cuestión que "constituye un elemento esencial de la protección de las personas en lo que respecta al tratamiento de datos personales" (considerando 62 de la directiva).

(30) Pueden verse críticas a esta opción en Renato Jijena L. "Transparencia, no Datos Personales", en La Tercera 29/06/2010 (http://latercera.com/contenido/895_271915_9.shtml). Dicha columna responde a una anterior de Juan Enrique Vargas V., que defiende la opción del CPT: "Transparencia y Datos Personales", en La Tercera 29/06/2010 (http://diario.latercera.com/2010/06/21/01/contenido/7_30413_9.shtml).

de un nuevo organismo a cargo de la protección de datos requeriría generar mecanismos para resolver posibles conflictos competenciales con el CPT. Sería indeseable que finalmente éstos escalaran a los tribunales, pues en tal caso se arriesgaría buena parte de la eficacia del modelo. Sin embargo, es inevitable que al final de la jornada existan muchos casos en que la resolución del problema de acceso a la información o *habeas data* en el ámbito de la administración pública requiera de una ponderación conjunta entre el derecho de acceso a la información pública y el derecho a la autodeterminación informativa. Si no tenemos una instancia administrativa única que lo haga, deberemos entregarle esta misión al Poder Judicial.

Otra conclusión nada de novedosa es que es preciso mejorar a la brevedad los estándares de la protección de datos personales en Chile. El ejemplo del CPT sugiere que la creación de una institución para la protección de datos, o la asignación de esta tarea al CPT, contribuiría notablemente a la difusión e implantación efectiva del derecho a la autodeterminación informativa. Probablemente también experimentaríamos una verdadera eclosión de este derecho, al modo de la vivida por el derecho de acceso a la información desde abril de 2008. Sin embargo, al margen de la discusión acerca del organismo encargado de esta tarea hay numerosos otros aspectos regulatorios que requieren de un perfeccionamiento, de manera que los ciudadanos tengan un control efectivo de sus datos y no sean "capturados" junto con ellos.

(...) al margen de la discusión acerca del organismo encargado de esta tarea hay numerosos otros aspectos regulatorios que requieren de un perfeccionamiento, de manera que los ciudadanos tengan un control efectivo de sus datos y no sean "capturados" junto con ellos.

Autor

Enrique Rajevic Mosler

Máster en Política Territorial y Urbanística, Profesor de Derecho Administrativo de la Universidad Alberto Hurtado y Director Jurídico del Consejo para la Transparencia.

La serie en foco recoge las investigaciones de la **Corporación Expansiva,** las que tienen por objeto promover un análisis interdisciplinario y riguroso sobre los temas fundamentales de la sociedad actual, con el fin de hacer propuestas que contribuyan a mejorar las políticas públicas del país.

Se agradece la participación de Raúl Arrieta como coordinador del proyecto que dio origen a este documento, así como el apoyo otorgado por el Comité de Retail Financiero. La presente versión fue editada por Daniela Crovetto y tanto ésta como todo el quehacer de Expansiva se encuentran disponibles en www.expansiva.cl