

Tratamiento de datos personales en el Estado y acceso a la información pública

*Personal data processing by the government and access
to public information*

RENATO JIJENA LEIVA

Escuela de Derecho, Pontificia Universidad Católica de Valparaíso

RESUMEN Ante la modificación del artículo 8 de la Constitución Política de 1980 y la promulgación de la Ley 20.285 sobre Transparencia y Acceso a la Información de los Servicios Públicos, ha surgido un nuevo mecanismo jurídico cautelar y procesal para ejercer el derecho de acceso ante los órganos del Estado y, en caso de negativa a la entrega de antecedentes, actos, contratos, documentos, resoluciones y contratos del Estado, acudirse de amparo ante el Consejo para la Transparencia. Empero, la vigencia anterior de la Ley 19.628 sobre Protección de la Vida Privada y el propio articulado de la Ley 20.285 —en materia de «transparencia activa» y de «causales de secreto o reserva»—, obligan fundadamente a que la protección legal del tratamiento de datos personales en los servicios públicos se constituya en una limitante al derecho de acceso a la información administrativa, máxime cuando la no necesidad de exigir expresión de causa o motivo para el solicitante es uno de los principios esenciales de la Ley 20.285.

PALABRAS CLAVE Protección de datos, datos personales, privacidad, acceso a la información pública.

ABSTRACT Before the amendment of Article 8 of the Constitution of 1980 and the enactment of Act 20 285, on transparency and access to information of public services, there is a new protective legal mechanism and procedures in order to exercise the right of access before the organs of state and, in case of refusal to the delivery of records, deeds, contracts, documents, resolutions and state contracts, go for defense before the Council of Transparency. However, the previous period of law 19.628 on protection of privacy and the actual wording of the law 20 285-on «active transparency» and «grounds of secrecy or confidentiality, to reasonably require legal protection treatment Personal data on public services should become a law limiting access to administrative information, especially when no need to require expression of cause or reason for the applicant is one of the essential principles of the law 20 285.

KEYWORDS Data protection, privacy, access to public information.

INTRODUCCIÓN

El artículo 33 letra m) de la Ley 20.285 sobre Acceso a la Información Pública (en adelante, indistintamente «Ley de Transparencia o «Ley 20.285») estableció, dentro de las competencias del nuevo órgano llamado Consejo para la Transparencia (en adelante, CPLT o Consejo, indistintamente), la obligación de velar por la aplicación y el cumplimiento de la Ley 19.628 que regula el procesamiento electrónico o manual (en adelante, indistintamente «Ley de Datos Personales» o «Ley 19.628») y la protección de datos personales o nominativos¹ en la gestión de los órganos de la Administración del Estado.

1. El artículo 2 contempla dos categorías, en relación de género a especie: i) los datos de carácter personal o datos personales, que son los relativos a cualquier información concerniente a personas naturales, identificadas o identificables; y ii) los datos sensibles, que son aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, «tales como» —dice la ley— los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.

Esta segunda normativa, titulada «Sobre protección de la vida privada» como consecuencia de un resabio de su tramitación parlamentaria, pero que no define los conceptos de vida privada, de privacidad o de intimidad y que se circunscribe sólo al ámbito del tratamiento de datos personales para asegurar el derecho al control y a la autodeterminación informativa que poseen sus titulares, es el resultado de una política pública y de una filosofía radicalmente diversa a la de la ley de acceso y transparencia a los actos y documentos de la Administración.²

Al decir del artículo 1, se sujeta a la Ley 19.628 el tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares.³ Ergo, al ser subsumida la aplicación de la Ley 19.628 dentro de la competencia de derecho público del Consejo para la Transparencia, lleva necesariamente a visualizar que al dedicarse a cumplir con el cometido el órgano de la transparencia y el acceso deviene —preliminarmente— en un garante de la intimidad de los ciudadanos, tanto en cuanto —la intimidad o privacidad— datos personales tratados⁴ computacionalmente por los servicios públicos.

Porque, como ha dicho un autor recientemente, uno de los desafíos del Consejo en la aplicación de la ley de acceso y transparencia es el de

2. Se le ha denominado (en el número 4 del artículo 1 de la Ley 20.285), por sus contenidos, la «Ley de Transparencia de la Función Pública y de Acceso a la Información de la Administración del Estado», y se mencionan como aspectos concretos esenciales de ella: i) las normas sobre transparencia activa, ii) la regulación de la transparencia pasiva o del ejercicio del derecho de acceso (que no es el *habeas data* de la Ley 19.628) y iii) la perspectiva orgánica o la creación del Consejo de Transparencia.

3. La excepción está dada (según el mismo artículo) por el tratamiento que se efectúe en ejercicio de las libertades de emitir opinión y de informar, que se regulará por la ley a que se refiere el artículo 19 número 12 de la Constitución Política. En este estudio se alude frecuentemente a la sigla «STDP», esto es, al Sistema de Tratamiento de Datos Personales que existe en toda corporación, servicio público, entidad o empresa.

4. La expresión tratamiento de datos personales está definida legalmente en Chile desde el año 1999, y es mucho más amplia que la referencia a las operaciones de recogida, procesamiento y almacenamiento de antecedentes nominativos. Legalmente, la expresión tratamiento alude a 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.

«generar criterios y mecanismos que puedan ser utilizados por los diversos órganos de la Administración del Estado para proteger la privacidad de terceros» (Soto Velasco, 2009: 10).

Todo servicio público, exclusivamente para cumplir sus funciones, requiere administrar y procesar computacionalmente antecedentes personales o nominativos de sus nacionales. Se requiere, por ejemplo, que el Estado pueda conocer sus rentas y su situación familiar para asignar subsidios, pensiones o beneficios de educación, sus datos de salud para fijar políticas públicas asistenciales, sus domicilios para ser notificados o determinar donde les corresponde votar, sus propiedades para aplicarles el impuesto territorial, o las importaciones y exportaciones que realizan las empresas para el cobro de aranceles aduaneros.

Son adecuadas las constataciones que se han hecho en cuanto a que el Estado es el principal tenedor de información personal (posee lo que la Ley 19.628 denomina «registros, recopilaciones o bancos de datos»⁵), ya que, efectivamente, i) por razones de planificación, gestión y orden público, almacena y registra hechos y documentos que constituyen información personal de los ciudadanos; ii) porque el Estado realiza tratamiento de datos personales sin necesidad de autorización expresa de los ciudadanos titulares sino por mandato legal; iii) porque se requiere manejar y procesar información nominativa al elaborarse políticas públicas y al desempeñar sus funciones los servicios públicos; y, iv) porque el Estado trata o procesa electrónicamente datos sensibles como los antecedentes de salud.

Al derecho público le corresponde establecer «límites» y «restricciones». Los primeros, para que no se vulnere la intimidad de las personas cuyos datos se procesan. Las segundas, para que sólo se usen los datos personales dentro de la competencia exclusiva de los servicios públicos y para sus fines específicos.

Resulta procedente hablar de la regulación jurídica de los Sistemas

5. Dice el artículo 2 letra m), que registro o banco de datos es el conjunto organizado de datos de carácter personal, sea automatizado o no y cualquiera sea la forma o modalidad de su creación u organización, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos. Luego, a modo de sinónimo, el artículo 11 alude a «registros o bases» de datos. En teoría general de sistemas un «banco» de datos es un «conjunto de bases de datos».

de Tratamiento de Datos Personales (STDP) en el sector público, porque conceptualmente —en el ámbito de la teoría general de sistemas— existen diversos componentes que conforman un todo cuando los órganos de la Administración utilizan las herramientas de la informática y de la telemática para gestionar los antecedentes nominativos de los ciudadanos y, en definitiva, cumplir sus fines promocionales y asistenciales.

Son diversas las normas legales generales y especiales, reglamentarias y administrativas que, sumadas a dictámenes de organismos fiscalizadores como la Contraloría General de la República, han configurado un marco de derecho público dentro del cual deben desempeñarse los órganos del Estado.

Si bien es cierto el énfasis del análisis se pone en la Ley 19.628 que regula a los servicios públicos en su calidad de «responsables de bases de datos» nominativos de los ciudadanos y de sus propios funcionarios, a partir de ella se puede realizar el cruce con otras normas relacionadas.

Así por ejemplo: i) puede encuadrarse en la Ley 19.628 la regulación legal de los datos llamados «RUN» y «RUT»; ii) se deben analizar los convenios de intercambio, cesión o comunicación de información nominativa entre servicios públicos o entre éstos y empresas particulares, dictaminados en cuanto a su validez por la Contraloría General de la República; iii) puede proyectarse la problemática del tratamiento de datos personales de los ciudadanos al uso de Internet, lo que lleva a revisar el Decreto Supremo 100; iv) cabe analizar el marco normativo relacionado con la seguridad que deben observar los servicios públicos en la gestión de los STDP, y un Decreto 83 que complementa lo establecido en la Ley 19.628; etcétera.

En este estudio se busca conciliar el marco normativo de los STDP con las disposiciones y contenidos de la Ley 20.285, con el criterio que deriva de entender que el tratamiento de los datos personales de los ciudadanos es y debe ser, jurídica, constitucional y legalmente una limitante al ejercicio del derecho de acceso a los actos, contratos, documentos, resoluciones y procedimientos de la Administración del Estado.

Para ello, i) se analizan en forma comparada las normas constitucionales, las políticas legislativas y los conflictos jurídicos que pueden presentarse, tanto en el ámbito de la protección de datos personales como en el de la ley de acceso y transparencia; ii) se argumenta acerca de la hipótesis central de trabajo, a saber, que la protección legal de los STDP

es una limitante al derecho de acceso a la información administrativa; iii) se analiza la excepción a la transparencia activa del artículo 7 de la ley, constituida por los datos personales sensibles o personalísimos; iv) se estudian los derechos contemplados para los titulares de los datos personales en la Ley 19.628, visualizados como motivo o causa suficiente para que un tercero notificado en virtud del artículo 20 de la Ley 20.285 se oponga válida y fundadamente a la solicitud de acceso; v) se analizan las causales de secreto o reserva de los números 2 y 5 del artículo 21, siempre en concordancia con la Ley 19.628; y, vi) se discurre luego acerca de la incompatibilidad entre el principio de la no exigencia de motivo o causa en las solicitudes de acceso de la Ley 20.285, con los supuestos esenciales de la Ley 19.628.

NORMAS JURÍDICAS GENERALES Y ESPECIALES QUE REGULAN LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES EN EL SECTOR PÚBLICO

Todo órgano de la Administración del Estado procesa datos personales o nominativos, públicos o secretos —así calificados por ley—, sobre personas naturales o jurídicas, nominados e innominados o estadísticos, que son recopilados o generados, procesados, almacenados y transmitidos en el ejercicio de sus funciones y competencias legales.

Por información estadística deben entenderse aquellos datos recopilados o generados que por su naturaleza no permiten individualizar a los ciudadanos, sean personas naturales o jurídicas; por información innominada, aquel conjunto de datos reales que se independizan de toda identificación o caracterización del administrado porque son disociados; y por información nominativa o datos personales, a aquellos que nominada e individualmente permiten determinar con precisión los antecedentes personales de los ciudadanos, tales como los llamados «datos de identificación del sujeto» (RUT, nombre, dirección, comuna, teléfono, fax o correo electrónico).

Las normas legales generales y particulares vigentes en Chile están llamadas a regular y a determinar los parámetros constitucionales y administrativos para el tratamiento y/o procesamiento computacional de los datos y de la información sobre los ciudadanos, que a un servicio público le compete recopilar, procesar, almacenar, generar y difundir en el cumplimiento de sus funciones públicas y únicamente en este ámbito.

Si las bases de datos de los servicios públicos no pueden ser calificadas como fuentes públicas de información, susceptibles de ser accedidas por cualquier particular, empresa o servicio público, en cualquier tiempo y en forma gratuita, salvo en condiciones y circunstancias excepcionales (si lo hubiese establecido una ley general u ordenado una resolución judicial), un órgano de la Administración sólo debiera permitir el acceso a los antecedentes o datos personales que recopila, procesa y genera: i) a los servicios públicos, a los tribunales y a las entidades facultadas por ley; y ii) a los propios ciudadanos titulares y propietarios de los antecedentes (personas naturales o jurídicas) a quienes se refieran o aludan, únicos requirentes frente a los cuales siempre puede hablarse de la existencia de una obligación legal —o carga pública— de entrega de información nominativa.

Toda evaluación por un servicio público para proceder a la entrega de información nominativa, que le pertenece a los ciudadanos y que sólo posee como mero tenedor para cumplir sus fines promocionales y asistenciales, siempre debiera considerar: i) la naturaleza concreta de los requirentes;⁶ ii) la naturaleza de la información solicitada (pública, privada, secreta o reservada,⁷ nominativa, estadística o disociada, relacionada, etcétera); iii) si existe —o no— una obligación expresa establecida

6. Esto, por cuanto las solicitudes o requerimientos de información nominativa pueden ser provenientes de diversas entidades, públicas y privadas, y personas jurídicas o naturales. En atención a su naturaleza, los solicitantes de información o datos personales, por ejemplo, pueden ser: i) el titular respecto de sus propios antecedentes que lo individualizan e identifican; ii) un ciudadano respecto de los antecedentes de terceros o ciudadanos distintos del peticionario; iii) los tribunales de justicia; iv) otro servicio público para el adecuado cumplimiento de sus fines y actuando dentro de su competencia; v) una empresa comercial de información sólo con fines de lucro; o vi) una empresa que excepcionalmente y por motivos calificados haya suscrito previamente un convenio de intercambio de información.

7. Así, por ejemplo, la situación más conocida e importante de información sujeta a secreto o reserva es el inciso segundo del artículo 35 del Código Tributario establece, para todos los funcionarios —sin excepciones—, la obligación de no divulgar, en forma alguna, la cuantía o fuente de las rentas y el capital efectivo de un contribuyente, ni las pérdidas, gastos o cualquier dato relativo a ellas, que figuren en las declaraciones obligatorias presentadas por los ciudadanos. Agrega que los funcionarios no podrán permitir que las declaraciones, sus copias o los libros o documentos que contengan extractos o datos tomados de ellas sean conocidos por persona alguna ajena al servicio.

por ley para proceder a la entrega de la información;⁸ y iv) «la finalidad de los requerimientos de datos o información personal», por cierto, una de las diferencias esenciales con los presupuestos de la Ley 20.285, que cuando nos trasladamos al ámbito del acceso y transparencia a la información administrativa (que documentalmente puede comprender o referirse a datos personales), expresamente prescinde de la exigencia de motivo o causa en una solicitud.

Y para este análisis, pero desde la perspectiva jurídica, toda evaluación para proceder a la entrega de información nominativa deberá considerar los siguientes criterios o niveles:

- Primero, estudiar la procedencia o no teniendo presente lo que establezcan normas legales generales de derecho público, como la Ley General de Bases de la Administración del Estado. Así, por ejemplo, en el caso que los requerimientos provengan de un servicio público, y en orden a contribuir con los restantes entes de la Administración del Estado en la prestación de los servicios públicos, por regla general el órgano de la Administración apoyará su gestión, toda vez que rige en este ámbito el principio de actuación coordinada de los órganos de la Administración del Estado establecido en el artículo 5 de la Ley 18.575.⁹
- Segundo, considerar lo que dispongan normas legales especiales o relacionadas con la naturaleza específica de la gestión del servicio público, como sus propias leyes orgánicas. Por cierto, tratándose

8. Un ejemplo de cuando el requirente es un servicio público facultado legalmente lo encontramos en el artículo 2 letra i) de la Ley 19.913 del año 2003, que al crear la UAF o Unidad de Análisis Financiero le asignó competencia para acceder a la información y a los antecedentes en poder de otros organismos públicos, pero con restricciones: que se trate de la revisión de una operación sospechosa previamente reportada a la UAF o detectada por ella en el ejercicio de sus atribuciones, salvo que se trate de información legalmente sujeta a secreto o reserva.

9. No obstante que se tenga presente la importancia de colaborar con los servicios públicos apoyando su gestión con el acceso a la información que les sea de utilidad, siempre debiera evaluarse que la solicitud de dicha información sea precisamente para el cumplimiento de los fines públicos que sean de su competencia y no por otras razones o para otros fines, porque lo que establece la LGBAE no es un derecho absoluto y posteriormente no podría excusarse el órgano requerido de no haber sido diligente en la aceptación de la solicitud.

de servicios públicos habilitados especial y expresamente por ley para acceder a la información del órgano de la Administración, y sin que ello implique desconocer el mandato de la ley, siempre debiera suscribir con tales servicios un convenio que determine las modalidades operativas y las medidas concretas de seguridad mediante las cuales se apoyará la gestión del órgano y se cumplirá con el mandato legal.

- Tercero, revisar luego lo que dispongan normas especiales como la Ley 19.628¹⁰ y la Ley 20.285¹¹ si es que éste fuera el contexto específico de la solicitud, porque los datos solicitados se contienen en un acto, contrato, resolución o documento administrativo.

La consecuencia de actuar en conformidad a estos criterios jurídicos es que podrá determinarse —siempre— la naturaleza posible de los datos o de la información que se esté solicitando; la competencia del servicio público para tratar, procesar, almacenar, generar o difundir los datos personales sobre los ciudadanos;¹² la naturaleza de la entidad que solicita información y los fines con que se hace; y, por último, incluso la determinación si es conveniente o no —lo que implica un análisis de mérito ineludible para el órgano de la Administración cuando se trata de la gestión diligente de datos personales— para los fines y funciones

10. Así, por ejemplo, si lo que está en juego es la petición de los antecedentes de salud de los chilenos que tienen sida al ministerio respectivo, debe entenderse que el artículo 10 de la Ley 19.628 establece que los datos sensibles no pueden ser tratados si una ley no lo autoriza, y cuando la ley orgánica del ministerio lo permite para sus funciones de un servicio público que actúa dentro de su competencia, ello no significa que los datos sobre los enfermos de sida pueden ser transferidos o comunicados a terceros libremente, si es que ésa no es una de las competencias específicas establecidas por ley para este órgano determinado.

11. En el mismo ejemplo de la petición de los antecedentes de salud de los chilenos que tienen sida al ministerio respectivo, en conformidad al artículo 21 número 2 de la Ley 20.285 se trataría de información sujeta a secreto o reserva por ser parte de la esfera privada de las personas.

12. En el cumplimiento de las funciones de su competencia de Derecho Público, el órgano público sólo puede recibir y procesar o generar información sobre los ciudadanos en la medida que una norma legal expresamente lo faculte al efecto, información nominativa que, por cierto, es recibida por diversos canales, tales como declaraciones en papel y electrónicas, llenado de formularios, solicitudes de beneficios sociales, etcétera.

del servicio público y de la Administración del Estado el entregar o no determinada información nominativa.

Todo órgano de la Administración debe tener presente que los ciudadanos poseen los mecanismos legales para controlar el uso respecto de los datos personales o nominativos que los individualicen, y que cualquier particular puede presentar una denuncia ante los Tribunales o ante la Contraloría General de la República. Tal derecho de petición está consagrado, de manera general, en la Constitución, en la Ley de Bases de la Administración del Estado y —ahora en concreto y de manera especial— en el artículo 12 de la Ley 19.628 y —desde el año 2008 pero sólo en cuanto se pida el acceso a actos, contratos o documentos del Estado y lo haga el propio titular de los datos personales— en el artículo 10 de la Ley 20.285.¹³

En su calidad de responsable de las bases de datos en las que se procesa, almacena y genera información, un servicio público debe dar cumplimiento cabal a todo requerimiento que una persona natural —titular de los datos— haga invocando como fundamento el derecho de acceso a antecedentes personales o datos nominativos que lo identifican, a que aluden los artículos 12 y 16 de la Ley 19.628.

El ciudadano-persona natural podrá solicitar información sobre la procedencia de los datos almacenados, el propósito de dicho almacenamiento, la identidad de los posibles destinatarios a los cuales los datos se les transmitan regularmente. Consecuencialmente, podrá pedir que ellos sean corregidos, actualizados, eliminados o bloqueados, salvo que con la petición se impida o entorpezca el debido cumplimiento de las funciones del servicio público, se afecte la reserva o secreto establecidos legalmente, o se afecte la seguridad de la nación o el interés nacional.

Existen una serie de normas legales generales y particulares, reglamentarias, administrativas y dictámenes de la Contraloría General de la República relacionados con la gestión de sistemas informáticos, de bases

13. Esto, con las particularidades o complicaciones que derivan que esa ley permite que cualquiera y no sólo un titular de datos solicite el acceso respecto de sus propios antecedentes personales, y que además lo puede hacer sin expresar motivo o causa. Debe concluirse la negativa de la solicitud en sede de la Ley 20.285, es nuestro parecer, si los datos personales no los pide el propio titular y si se piden sin expresión de causa o motivo.

de datos personales, de servidores y de redes telemáticas abiertas (como Internet) o cerradas (como las intranets o las redes VAN que operan en materia aduanera), que en su conjunto determinan la competencia, obligaciones y responsabilidad específica de un órgano de la Administración del Estado en materia de tratamiento informático y/o telemático de datos personales.

Por cierto, el conjunto de normas que habilitan y regulan el procesamiento electrónico de datos personales sobre los ciudadanos (personas naturales o jurídicas) son leyes que facultan a los servicios públicos para tratarlos sin el consentimiento expreso previo del titular, o desde ya, sin que se requiera la autorización previa de los titulares de los datos personales. Y esto, únicamente para posibilitar que ellos cumplan sus fines promocionales y asistenciales y para velar por un interés superior de orden público que los convoca y preside, porque de tratarse o procesarse los datos personales o nominativos de otra forma surgirán las diversas responsabilidades que más adelante se analizan.

Por lo mismo, determinar los criterios jurídicos aplicables, los deberes, las limitaciones y las responsabilidades de los funcionarios públicos, por un lado, y los derechos de los ciudadanos, por el otro, no se logra sólo con el análisis del articulado de la Ley 19.628.

Las normas legales generales y particulares, reglamentarias y administrativas referidas, por ejemplo, a la seguridad de sistemas, a la mantención de repositorios documentales, o al uso de Internet y de páginas web, en cuanto incidan en la gestión informática ajustada a derecho y diligente de los datos personales de los ciudadanos que por su naturaleza pueden ser tratados computacionalmente por uno o más servicios públicos, también configuran y/o determinan lo que el artículo 20 de la Ley 19.628 califica como «las materias de su competencia» exclusiva.¹⁴

Así, en concreto y, por ejemplo, cuando el artículo 33 letra m) de la Ley 20.285 establece que el Consejo para la Transparencia debe velar por el cumplimiento de la Ley 19.628 al interior de la Administración del Estado, por aplicación de un Decreto Supremo 100 del año 2006 la

14. Título IV: «Del tratamiento de datos por los organismos públicos»; artículo 20: «El tratamiento de datos personales por parte de un organismo público sólo podrá efectuarse respecto de las materias de su competencia y con sujeción a las reglas precedentes. En esas condiciones, no necesitará el consentimiento del titular».

competencia de vigilancia o tutela se extiende a la definición que se haga de las políticas de privacidad respecto de los datos personales de los ciudadanos disponibles, accedidos, recopilados y registrados mediante los sitios web de los servicios públicos.

NORMAS CONSTITUCIONALES, POLÍTICAS LEGISLATIVAS Y CONFLICTOS JURÍDICOS DIVERSOS. DISTINCIONES ESENCIALES ACERCA DEL CONTEXTO DE LAS LEYES 19.628 Y 20.285

En agosto del año 2008 se promulgó en Chile la Ley 20.285¹⁵ la que junto con crear un nuevo órgano llamado Consejo para la Transparencia, fue el resultado de una reforma constitucional previa.

La modificación a la Constitución Política del año 2005¹⁶ contempló la incorporación de un nuevo artículo 8,¹⁷ en cuya virtud y dentro del capítulo de las «Bases de la institucionalidad», se estableció, en primer lugar, que el ejercicio de las funciones públicas en Chile obligaba a sus titulares a dar estricto cumplimiento al principio de probidad en todas sus actuaciones.

En segundo lugar, se declaró perentoriamente que «son públicos»: los actos y las resoluciones de los órganos del Estado, sus fundamentos y los procedimientos utilizados, pudiendo establecerse por excepción y sólo mediante una ley de quórum calificado su reserva o secreto en consideración a cuatro determinadas y genéricas causales (lo que dejó sin respaldo legal a los múltiples decretos de reserva y secreto dictados en años anteriores y lo que demuestra que el derecho de acceso no es absoluto).

15. Véase <<http://www.habeasdataorg.cl/2008/07/28/proteccion-de-datos-personales-a-proposito-de-la-transparencia-y-el-derecho-de-acceso-a-la-informacion-del-estado/>>.

16. La modificación se hizo en la misma época en que la Contraloría General de la República ya había consignado la existencia de aproximadamente cien resoluciones que establecían secreto o reserva de actos administrativos.

17. Por cierto, la importancia que le damos a la regulación constitucional no implica desconocer la relevancia de otros antecedentes previos, como la Ley de Probidad Administrativa de 1999 que incorporó a la LGBAE el Principio de Transparencia, o los debates y recursos presentados contra el secreto o la reserva administrativa definida libremente vía decretos, considerados aquellos desde siempre como la regla general, gracias al procedimiento administrativo de acceso a la información del Estado que también se creó en 1999 para el evento de que un servicio público se negara a entregar una información que le fuera solicitada.

Esta piedra angular vino a fortalecer, para los ciudadanos, el llamado derecho de acceso a la información relacionada con los actos y documentos de la Administración estatal consagrado previamente, en 1999, en la Ley General de Bases de la Administración del Estado.¹⁸ Y vino a aclarar que sólo el Congreso y no los propios entes u órganos públicos —como ocurría en el pasado— es el llamado a establecer «excepciones a la publicidad», es decir, hipótesis de reserva o secreto cuando ella afecte el cumplimiento de las funciones públicas, los derechos de las personas, la seguridad de la nación o el interés nacional.

Dentro de la causal «los derechos de las personas» caben los reconocidos por el artículo 19 número 4 de la Constitución y por la Ley 19.628 en el ámbito del tratamiento de datos personales o nominativos, que formen parte de la esfera y de la vida privada o íntima de una persona y de su familia. Esencial, genérica y principalmente, el derecho de acceder a ellos, de controlarlos y de autodeterminarlos al momento de su tratamiento o procesamiento —principal, pero no exclusivamente— electrónico, informático o telemático.

Por eso es dable sostener desde ya, sin entrar aún al análisis de la Ley 20.285, en general, y de su artículo 21 número 2 que alude a la esfera de la vida privada, en particular, que la protección legal de tratamiento de datos personales es una limitante al ejercicio del derecho de acceso a la información administrativa del artículo 10 de la Ley 20.285, ya que ellos, los datos nominativos, por regla general son protegidos constitucional y legalmente con una esfera de secreto o reserva.

En efecto, si el objetivo esencial de la ley de acceso y transparencia ha sido «abrir los espacios públicos al escrutinio ciudadano»; o, como consigna Soto Velasco (2009: 5), si «la letra y el espíritu de la ley están contruidos para incentivar la apertura y la transparencia en el ejercicio de la función pública», esa apertura, esa mayor sensibilización con la necesidad de exigirse y generarse rendiciones de cuentas ante la gestión de los servicios públicos, debe reconocer necesariamente límites y restricciones en la protección de la privacidad y de los datos nominativos de los mismos ciudadanos.

18. Las expectativas son altas, sobre todo si diversos autores le asignan a la transparencia un rol clave para el ejercicio de los derechos de las personas, para la modernización del Estado y para el perfeccionamiento de la democracia.

Desde la perspectiva de las garantías constitucionales en juego, cabe visualizar la necesidad de armonizar tres de ellas: la del artículo 19 número 4, la del artículo 19 número 12 y la del artículo 8. Entonces, la interrogante a dilucidar es la siguiente: ¿cómo conciliar el derecho a la información con el derecho a la intimidad?, ¿cómo equilibrar por un lado la máxima libertad o acceso a la información con un adecuado resguardo de la privacidad?

Se trata de una cuestión importante y no de meras disquisiciones teóricas o doctrinarias, porque si bien es cierto el orden público social y económico de una nación requiere que tanto el Estado como los particulares manejen, conozcan o accedan a determinados datos personales, sea por ejemplo el Ministerio de Salud para fijarse políticas o asignarse beneficios de salud (datos personales sensibles) —lo que expresamente le permite la Ley 19.397—, sea para evitarse la morosidad comercial (datos personales patrimoniales negativos), o sea para conocerse con transparencia la probidad de la gestión de los órganos de la Administración del Estado (información de la gestión pública), ello no puede traducirse, al extremo, en perjuicios contra las personas titulares e individualizados por sus antecedentes nominativos, personales y sensibles.

En Chile es el artículo 12 de la Ley 19.628 el que consagra el llamado derecho de acceso, *habeas data* o *habeas scriptum*, un derecho sólo de rango legal y procesal, aún no constitucional, que vino a desarrollar la garantía o el derecho público subjetivo del respeto —por la sociedad toda— y de la protección —por el ordenamiento jurídico— de la vida privada de la persona y su familia, que contempla y asegura para todas las personas el artículo 19 número 4 de la Constitución Política.

Por su intermedio cada titular puede requerir a quien sea el responsable de una base o banco de datos nominativos en un servicio público, conocer y corregir, modificar o actualizar la información computacional, tratándose de datos personales, nominativos, o relativos a cualquier información concerniente a personas naturales, identificadas o identificables, particularmente si son antecedentes sensibles o referidos a características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como —dice la ley— sus hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.

Y por su intermedio, se apunta sólo a un interés personal de control y autodeterminación, y nada se busca transparentar, en beneficio de la sociedad o para velar porque en el ejercicio de las funciones públicas se dé cumplimiento al principio de probidad del artículo 8 de la Constitución.

Acceso para la transparencia de la información administrativa versus acceso para la autodeterminación de la información nominativa. La distinción puede también conceptualizarse desde el análisis de los diversos alcances del derecho de acceso a la información.

Hasta la fecha, el mayor grado de sensibilización en cuanto a las necesidades de acceso a la información derivaba del ejercicio profesional de los periodistas y los medios de comunicación social, tema que está regulado en Chile por la Ley 19.773 sobre Libertad de Opinión e Información.

Pero el derecho a la información puede ser enfocado desde otras dos perspectivas, a saber, i) la de los ciudadanos que quieren acceder a los documentos que almacenan y generan los órganos del Estado, los que en Chile se deben transparentar activa o pasivamente con fines de probidad en virtud de la Ley 20.285, y, ii) la de la posibilidad de que las personas controlen, autodeterminen y accedan a todos aquellos datos personales o nominativos que les afecten por referirse a ellos, a su vida privada, a su intimidad o privacidad, sean procesados manual o electrónicamente tanto por órganos públicos como por empresas particulares.

Dicho de otra forma: i) una perspectiva —la de la Ley 20.285— apunta al objetivo de accesar actos administrativos, contratos administrativos, documentos y resoluciones, para generar transparencia y publicidad ante el requerimiento de cualquier ciudadano y sin expresión de causa o motivo; ii) la otra —la de la Ley 19.628— busca acceso para asegurar el control, la autodeterminación y la reserva de los datos o antecedentes nominativos de una persona determinada, legitimada activamente por estar en juego sus propios antecedentes personales, que le pertenecen y que lo identifican actualmente o lo hacen identificable a futuro.

Citados a exponer frente a la Comisión de Economía de la Cámara de Diputados con ocasión de la tramitación del Boletín 6120 en curso, modificatorio de la Ley 19.628, planteamos la necesidad de una distinción esencial.¹⁹ A saber, que el derecho de acceso que todos los ciudadanos para conocer los actos, contratos y documentos de los órganos de la

19. Exposición disponible en <<http://www.derecho.ucv.cl/jijenacam.pdf>>.

Administración del Estado (y que es el ámbito de acción principal del Consejo para la Transparencia a esta fecha), es radicalmente distinto al derecho de acceso o *habeas data* que posee desde 1999 toda persona para controlar y autodeterminar el uso y el eventual abuso únicamente de sus datos y antecedentes personales y nominativos, al tenor de las disposiciones de la Ley 19.628. Dicho de otra forma: porque asegurar la «transparencia activa» que exige la Ley 20.285 en el ámbito de protección de datos personales no existe; al contrario, acá, para garantizar el respeto del artículo 19 número 4 de la Constitución debe evitarse el libre flujo de datos personales que no sean públicos o provenientes de fuentes públicas, y cuyo tratamiento no esté autorizado o por el propio titular o por la ley en forma supletoria de su voluntad.

Hicimos presente que lo que está en juego en el actual debate parlamentario es el tema de defender una garantía fundamental —el artículo 19 número 4, el respeto y protección de la vida privada de las personas y sus familias—, que legalmente en Chile y de cara al procesamiento computacional de datos personales o nominativos, fue protegida con falta de idoneidad el año 1999 por la Ley 19.628, lo que, por cierto, se hace mucho más patente en el sector privado que en el sector público. Por eso, además, planteamos que sería importante que en paralelo avanzara la moción que busca la constitucionalización del *habeas data*, porque éste es el real nivel de protección jurídica —el de rango más alto en la pirámide normativa— que se necesita del ordenamiento jurídico chileno en materia de tratamiento de datos personales. En concreto, se propone:

Artículo único: Modifícase el artículo 19 número 4 de la Constitución [...] agregándose los siguientes incisos segundo y tercero:

Toda persona tiene derecho a la protección de sus datos personales, los que deben ser tratados para fines concretos y específicos, con su propio consentimiento, o en virtud de otro fundamento contemplado en la ley, y tendrá, asimismo, derecho a acceder a dichos datos, para obtener su rectificación, actualización o cancelación, según procediere

Una ley orgánica constitucional establecerá las normas para la debida aplicación de este derecho, como asimismo el órgano autónomo que velará por el cumplimiento de dicha ley y controlará su aplicación.²⁰

20. Disponible en <<http://www.habeasdataorg.cl/2008/06/05/%C2%BFhacia-la-constitucionalizacion-del-habeas-data-en-chile/>>.

LA PROTECCIÓN LEGAL DEL TRATAMIENTO DE DATOS PERSONALES EN LOS SERVICIOS PÚBLICOS DEBE CONSIDERARSE COMO UNA LIMITANTE AL DERECHO DE ACCESO A LA INFORMACIÓN ADMINISTRATIVA

Debemos ahora circunscribirnos a la necesidad de determinar y conciliar las relaciones existentes entre el llamado derecho de acceso a la información del Estado, que es el ámbito de las normas y principios del artículo 8 de la Constitución y de la Ley 20.285, con el llamado derecho de acceso o *habeas data* que cada persona posee para proteger su privacidad, controlar y autodeterminar el uso y el procesamiento de sus datos personales o nominativos, porque le pertenecen y porque lo identifican o individualizan, derecho regulado constitucionalmente por el artículo 19 número 4 de la Constitución y por la Ley 19.628.

Porque el derecho de acceso que todos los ciudadanos poseen reconocido constitucional²¹ y legalmente para conocer los actos, contratos, resoluciones y documentos del Estado, sin que se les exija expresión de causa o motivo, es radicalmente distinto al derecho de acceso o *habeas data* que debe poseer toda persona para controlar y autodeterminar el uso y el eventual abuso sólo o exclusivamente de sus propios datos y antecedentes personales o nominativos.

Hay algunas ideas centrales o propuestas sobre las cuales se hace necesario reflexionar y, en la medida de lo posible, consensuar un criterio, de cara al necesario equilibrio o conciliación, tales como:

- La protección de datos personales de los ciudadanos (y de los propios funcionarios públicos) debe ser un límite al derecho de acceso a la información, pero considerando caso a caso y la especial naturaleza del dato personal involucrado.
- Las leyes de acceso a la información necesariamente deben ser compatibles con las de privacidad y datos personales.
- La protección de datos personales no debe usarse «de manera general y sistemática» para no abrir información del Estado, ya que la restricción al acceso de ciertos y determinados antecedentes re-

21. Nota del Editor: sobre el alcance del artículo 8 de la Constitución, véase el considerando decimoquinto de la sentencia del Tribunal Constitución rol 2153, de once de septiembre de 2012.

feridos a los ciudadanos y a los funcionarios públicos puede amparar actos de corrupción, lo que, por cierto, también debe resolverse caso a caso o en forma individual según la especial naturaleza del dato personal pedido de acceso.

En Chile resulta clave definir hasta dónde llega o cuál es el alcance jurídico de la referencia a «todo otro tipo de información que obre en poder de la Administración o que sea elaborada con fondos públicos», de los artículos 5 y 10 de la Ley 20.285, para entender —o no (que es nuestro parecer)— que los datos personales *per se* no se deben considerar incluidos junto a los actos, contratos, resoluciones, procedimientos y documentos que deben ser públicos al estar en poder de los servicios públicos y accesibles para cualquier persona que los solicite, sin expresar causa o motivo legítimo.²²

La misma idea aparece en el artículo 11, que consagra en la letra c) el principio de apertura o transparencia, conforme al cual «toda la información en poder de los órganos de la Administración del Estado» se presume pública, salvo leyes de quórum calificado que establezcan lo contrario. Esta presunción de publicidad no puede extenderse, con fundamento jurídico serio, a los datos personales o nominativos.

Si a un servicio público se le solicitan directamente los nombres de los habitantes de una comuna, sus domicilios, sus direcciones de correo electrónico, sus profesiones, sus propiedades o sus estados de salud la respuesta debiera ser el rechazo, por tratarse de datos personales excluidos de las causales de solicitud, antes de entrar al análisis de fondo en cuanto a la procedencia de la causal de reserva del artículo 21 número 2.

Lo anterior puede ser expresado a modo de fórmula: si dado lo que disponen el artículo 8 de la Constitución, el artículo 7 letra i), el artículo 21 números 2 y 5 y el artículo 33 letra m) de la Ley 20.285, se concluye que el Constituyente y el legislador fueron sensibles a la necesidad de proteger los datos personales y en definitiva la privacidad de los administrados. El alcance de los artículos 5 y 10 de la misma ley no puede interpretarse de manera que se subsuma dentro de la información que deba transparentarse, entregarse sin motivo o causa o publicarse, los da-

22. Es, por cierto y lo repetimos, y salvo error u omisión, una discusión que no se presentó ni se resolvió durante el debate parlamentario que originó la ley 20.285.

tos nominativos de los ciudadanos, que no serían una especie de aquella «toda otra información que obre en poder de los órganos de la Administración» o de aquella referida como «toda información elaborada con presupuesto público».

Es clave pues, lo reiteramos, definir hasta dónde llega o cuál es el alcance jurídico de la referencia a «todo otro tipo de información que obre en poder de la Administración o que sea elaborada con fondos públicos», de los artículos 5 y 10, para decidir si hacemos primar o no la normativa sobre derecho de acceso por sobre la confidencialidad y restricciones que establece la Ley 19.628 para proteger a los titulares de los datos personales procesados computacionalmente —incluso con una carga legal expresa de secreto en su artículo 7—, sean dichos datos de los ciudadanos, sean de los propios funcionarios públicos.²³

Pero a las dos posibles interpretaciones anteriores que no compartimos (entender que prima la Ley 20.285 y que dentro del concepto de «información del Estado» caben los datos personales de los ciudadanos), se oponen, en nuestra opinión, los artículos 7 letra e), 21 número 2, el 21 número 5, el 33 letra m) de la Ley 20.285, los artículos 8 y 19 número 4 de la Carta Fundamental y la Ley 19.628, que obligan a que se protejan los derechos de las personas y la esfera de su vida privada y a que se respete la Ley 19.628 en el sector público, debiendo precisamente velar el Consejo para la Transparencia por su cumplimiento y aplicación.

Adicionalmente —es otro argumento—, si retomamos el inciso segundo del artículo 5 de la Ley 20.285 cuando establece que «es pública toda otra información que obre en poder de los órganos de la Administración», y tenemos presente la definición esencial del contenido del principio de transparencia del inciso segundo del artículo 4,²⁴ debe concluirse que sólo será pública la información administrativa que por su naturaleza sea factible de «facilitarse su acceso» a cualquier persona, sin

23. Téngase presente que, en relación a los funcionarios públicos, vía transparencia activa se publican sus remuneraciones, que ellas no se asocian a los RUT, y que en sede de transparencia pasiva el Consejo a esta fecha ha resuelto entregar sus calificaciones.

24. La norma señala que el principio de transparencia de la función pública consiste en respetar y cautelar la publicidad de los actos, resoluciones, procedimientos y documentos de la Administración, así como la de sus fundamentos, y en facilitar el acceso de cualquier persona a esa información, a través de los medios y procedimientos que establezca la ley.

que se le exija a ella expresión de causa o motivo al solicitar conocerla. Pues bien, esta condición no concurre respecto de los datos personales o nominativos de los administrados que sean tratados por los servicios públicos,²⁵ porque ellos, por regla general y en conformidad al artículo 12 de la Ley 19.628, sólo son accesibles para su propio titular, y porque a su respecto existe —para los responsables del tratamiento en el órgano administrativo— la obligación general de secreto del artículo 7 de la misma ley.

Por todo lo dicho, no es dable compartir que se considere que cuando un titular de datos personales ejerza el *habeas data* procesal del artículo 12 de la Ley 19.628 ante el responsable del registro o banco de datos de un servicio público, para o con la finalidad de controlar y autodeterminar el tratamiento sólo de sus propios datos nominativos —en definitiva, para velar por la protección de su privacidad o intimidad—, existiría jurídicamente «coincidencia eventual» con las causales de acceso del artículo 10 de la Ley núm. 20.285.²⁶

El acceso a la información administrativa además puede ejercerlo cualquier persona y no sólo el titular de los datos personales, y este principio es inaceptable en el régimen de la Ley 19.628.

Menos fundamento jurídico posee afirmar que el acceso de la Ley 20.285 tendría un carácter «general» y que el *habeas data* de la Ley 19.628 sería una «particularidad» (¿o especie?), cuando ocurre que su

25. La excepción estará dada por los datos personales que provengan de fuentes públicas a cuyo respecto el servicio público tenga competencia para darlos a conocer, o cuando estemos frente a datos personales contenidos en documentos como certificados o resoluciones que, también por ley, sea de la competencia exclusiva del servicio público el emitirlos (Registro Civil, Tesorería General de la República, Aduana, Servicio de Impuestos Internos, etcétera).

26. Véase la propuesta en <http://www.consejotransparencia.cl/prontus_consejo/site/artic/20091214/pags/20091214173541.html>. La propuesta concretamente se fundamenta de esta manera: «Lo anterior, pues el artículo 10 de la Ley de Transparencia dispone que ‘Toda persona tiene derecho a solicitar y recibir información de cualquier órgano de la Administración del Estado, en la forma y condiciones que establece esta ley’. Y agrega que ‘El acceso a la información comprende el derecho de acceder a las informaciones contenidas en actos, resoluciones, actas, expedientes, contratos y acuerdos, así como a toda información elaborada con presupuesto público, cualquiera sea el formato o soporte en que se contenga, salvo las excepciones legales’».

naturaleza jurídica, sus requisitos de procedencia, su objeto, su ámbito de aplicación y su fundamentación son totalmente distintos.

Dicho de otra forma: no tienen por dónde coincidir jurídicamente, y esa atribuida generalidad no puede —con fundamento claro, apoyándose en el análisis del debate parlamentario o en la historia de la ley— incluir a los datos personales o nominativos en los artículos 4, 5 y 10 de la Ley 20.285, sea que los solicite un tercero sin motivo o causa, sea incluso que los requiera su propio titular en el contexto de la ley de acceso y transparencia.

También resulta cuestionable sostener —como se hace en la misma propuesta en comento— que lo que encarga la Ley 20.285 y el artículo 8 de la Constitución al Consejo para la Transparencia es la competencia de velar por un «acceso universal a la información», tanto a una que se califica de «naturaleza privada» y a la que sólo podría tener acceso el titular para el ejercicio de sus derechos, como a una llamada «de naturaleza pública».²⁷

Es efectivo que el artículo 33 letra m) lleva al Consejo a velar porque los servicios públicos cumplan con la Ley 19.628 en materia de protección de datos personales,²⁸ pero esta facultad, como veremos, se contempló o se agregó en forma paralela o al margen de la previa institucionalidad del acceso a la información de la gestión del Estado cuya probidad se busca controlar, y no se puede extender al punto de considerar que estamos —en virtud del sólo artículo 33 letra m)— frente a la nueva Autoridad o Agencia de Protección de Datos chilena y que el Consejo, por ende, tenga competencia procesal y administrativa para conocer de reclamos en que se invoque la no aplicación o respeto de la ley 19.628.

La posibilidad legal concreta para que sólo su titular acceda a datos personales tratados por los servicios públicos y solicite conocerlos e incluso su eventual rectificación, modificación, cancelación, eliminación o

27. Cuándo una información sería de naturaleza «pública» y cuándo «privada» es algo que los abogados que formulan la propuesta no aclaran en forma debida y que se hace necesario.

28. Y así, por ejemplo, debiera instruir para que los servicios fueran ágiles al contestar los *habeas data* del artículo 12 antes de las 48 horas o de los dos días hábiles que establece el artículo 16 de la Ley 19.628 y de que el ciudadano recurrente acudiera a los tribunales.

bloqueo es la vía de la Ley 19.628, y cualquier servicio público al que se recurra con este único objetivo invocándose el artículo 10 de la Ley 20.285 y luego el Consejo conociendo del eventual amparo de acceso del artículo 24, debieran rechazar la solicitud por no tratarse de la vía jurídica idónea por medio de la cual recurrir. Más que ser complementarios ambos derechos de acceso, lo que jurídicamente ocurre es que el *habeas data* de la Ley 19.628 prima por especialidad, y que el acceso de la Ley 20.285 no es una acción amplia o «universal» que pueda sustituir o comprender a la anterior.

Otra cosa es —porque cambia el escenario del análisis— si se solicita el acceso a un concreto acto administrativo que en su contenido tenga datos nominativos de una persona natural o de una persona jurídica (por ejemplo, la asignación de una pensión de salud, la designación de un postulante a un cargo público, la aplicación de una sanción administrativa, la adjudicación de una licitación, etcétera).

Por cierto, a esta fecha el Consejo ha considerado tener competencia para conocer del reclamo respecto de los datos personales de un solicitante, con la particularidad de que no era un tercero cualquiera que accionara sin expresar causa o motivo (como lo permite el artículo 11 letra g) de la Ley 20.285), sino que era el propio postulante y titular de los datos el que quería acceder a los resultados de su evaluación personal.

Dichos exámenes además habían sido parte de los fundamentos tenidos en vista en un proceso administrativo de postulación a un cargo en un servicio público —que podría no haber sido transparente o probo y a cuyo respecto se buscaba publicidad—, y concretamente para la dictación del acto administrativo final de selección.²⁹ En este particular y excepcional caso,³⁰ al solicitante y recurrente de amparo no podría aplicársele la causal de reserva o secreto del artículo 21 número 2 porque

29. Véase la Decisión de Amparo A29-09 disponible en <www.consejotransparencia.cl>. En este caso, no se solicitaron en forma directa los datos personales sino el acceso a un acto administrativo, lo cual permitía aplicar el artículo 10 de la Ley 20.285

30. Caso en el cual, además, no se estaba invocando como fundamento de la petición de acceso la causal «cualquiera otra información que obre en poder del servicio o que se elabore con presupuesto público», sino en que se solicitó el acceso a un acto administrativo específico.

precisamente se trataba de sus antecedentes, y el Consejo determinó la procedencia de la entrega de la información.³¹

¿Pero si la solicitud de acceso a la información la hubiera presentado una persona distinta del titular de los datos, habría el Consejo aceptado la concurrencia de la causal del artículo 21 número 2³² y denegado el acceso a la información?

También será clave definir si las bases de datos de los órganos de la Administración son o no de aquellas fuentes públicas de datos personales que define la Ley 19.628, porque de serlo o de interpretarse a su respecto su libre disponibilidad o accesibilidad, se entendería —lo que sería inconstitucional e ilegal a nuestro parecer— que no existen restricciones legales para los servicios públicos que traten computacionalmente datos nominativos, como son, al tenor de la Ley 19.628, la obligación de guardar secreto del artículo 7 o la de usar los datos nominativos de los ciudadanos sólo para los fines que fueron recopilados, del artículo 9.

Todo lo anterior debe ser considerado antes y en paralelo o durante el cumplimiento de la obligación que recae sobre el Consejo para la Transparencia para, conociendo de un amparo al derecho de acceso, realizar lo que se ha denominado como un «test de transparencia, de interés público, de equilibrio o de daño»,³³ esto es, en esencia, balancear el principio de la proporcionalidad entre el interés que pueda existir para dar publicidad a una información administrativa determinada con el interés en mantenerla reservada o retenerla; o dicho de otra forma, se trata de «determinar si el beneficio público resultante de conocer la

31. Haciendo aplicación de la normativa relativa a la protección de datos, el Consejo determinó que es claro el artículo 2 letra ñ) de la Ley 19.628, sobre protección de datos personales, que entiende por titular a la persona natural a la que se refieren los datos de carácter personal, y que en consecuencia el requirente tenía derecho a conocer su evaluación personal, con excepción de las referencias de terceros.

32. Es la que permite negar el acceso cuando su publicidad, comunicación o conocimiento afecte los derechos de las personas, particularmente tratándose de su seguridad, su salud, la esfera de su vida privada o derechos de carácter comercial o económico.

33. Véase <http://www.redipd.org/reuniones/encuentros/IV/common/mexico_acceso_definitivo.pdf>, donde se encuentra el documento «Acceso a la Información Pública y Protección de Datos Personales», adoptado en México el año 2005 en el contexto del IV Encuentro Iberoamericano de Protección de Datos.

información solicitada es mayor que el daño que podría ocasionarse al ser ella revelada». ³⁴

Aplicado este recurso a la protección de datos personales, conceptualmente habría que usar el test sólo cuando en una solicitud de acceso a información administrativa se presente el caso que el documento, el acto, la resolución o el contrato contengan datos que sean de carácter personal, sensibles o nominativos, referidos tanto a una persona natural como a una jurídica y aun cuando la Ley 19.628 no ampara a las fictas sino sólo a las físicas, ³⁵ lo que obliga —al órgano requerido primero y sobre todo al Consejo para la Transparencia después— a decidir si prevalece la protección de la esfera privada —la causal del artículo 21 número 2 en concreto— o el interés público en dar a conocer la información solicitada.

Nosotros sostenemos que si el Consejo se enfrenta a la opción de resolver si es jurídicamente procedente dar a conocer una información administrativa que contenga datos personales o nominativos, ³⁶ o si de rechamente se piden tales datos en forma directa (por ejemplo, las direcciones o los domicilios de un funcionario público, los RUT de los propietarios asociados a los roles de avalúo de las propiedades que se poseen, ³⁷ los correos electrónicos de los ciudadanos, la nómina de enfer-

34. Decisión de Amparo A45-09.

35. Esto lo sostenemos porque la causal del artículo 21 número 2 no debería entenderse restringida sólo a la esfera privada de las personas naturales.

36. Un ejemplo: el Consejo de Transparencia ha ponderado ambos derechos en un amparo al derecho de acceso a la información interpuesto contra de la Dirección Nacional del Servicio Civil, que negó el acceso a la información relativa al proceso de selección implementado para proveer el cargo de Subdirector de Estudios y Desarrollo del Servicio de Registro Civil e Identificación (Decisión Amparo A35-09). Estimó que respecto de los dos postulantes que no se opusieron a la entrega de su identidad ni informaron el traslado conferido, podría aplicarse la obligación de secreto del artículo 7 de la Ley 19.628 declarando que sus identidades eran reservadas; pero optó por la publicidad, ya que el inciso final del artículo 20 de la Ley 20.285 dispone que de no deducirse oposición por parte de la persona potencialmente afectada por la difusión de una determinada información dentro de los tres días desde que fue notificada de la solicitud se entenderá que accede a la publicidad de dicha información. Lo anterior, por la especialidad otorgada a la ley de acceso y transparencia y por el interés público existente en conocer el funcionamiento del Sistema de Alta Contratación Pública.

37. Respecto a los datos sobre bienes raíces debe resguardarse la confidencialidad:

mos de sida, etcétera), y lo hace además un solicitante que no es el titular de los datos nominativos y que recurre de amparo al acceso sin haber expresado motivo, causa o legítimo interés, siempre debiera denegarse la solicitud y rechazarse el amparo, haciéndose primar la protección de la privacidad, i) en razón de la obligación de velar por el cumplimiento de la Ley 19.628 que es de competencia del Consejo, y ii) en virtud de la causal del artículo 21 número 2 de la Ley. 20.285.

LA PROTECCIÓN DE LOS DATOS PERSONALES-SENSIBLES DE LOS CIUDADANOS ES UNA EXCEPCIÓN A LAS NORMAS DE TRANSPARENCIA ACTIVA DEL ARTÍCULO 7 DE LA LEY 20.285

El título III de la Ley 20.285 se denomina «De la transparencia activa», y el artículo 7 establece expresamente que los órganos de la Administración del Estado señalados en el artículo 2,³⁸ deberán mantener a dis-

tanto de i) la información catastral asociada o conteniendo los datos relativos a roles de avalúo más nombre y/o RUT de los propietarios —lo que demuestra patrimonio y constituyen datos personales positivos sujetos a la obligación de secreto del artículo 7 de la Ley 19.628—; como ii) el resultado de asociar los datos de domicilio y roles de avalúo, por cuanto sin autorización previa de los ciudadanos tales antecedentes podrían usarse con el fin de realizar promociones comerciales.

Si bien es cierto en cada municipio pueden consultarse los roles de avalúo de cada comuna sin ser asociados a la identidad de los propietarios —porque deben ser publicados por ley—, es radicalmente distinto no entender que si otros servicios públicos en Chile si los poseen sistematizados y asociados a los datos de sus propietarios es únicamente para aplicar, determinar y cobrar el impuesto territorial, que es la finalidad de servicio público que genera la competencia de la TGR y del SII, y que a su respecto rigen obligaciones de secreto y de confidencialidad porque son datos personales o nominativos.

38. Señala: «Las disposiciones de esta ley serán aplicables a los ministerios, las intendencias, las gobernaciones, los gobiernos regionales, las municipalidades, las Fuerzas Armadas, de Orden y Seguridad Pública, y los órganos y servicios públicos creados para el cumplimiento de la función administrativa. La Contraloría General de la República y el Banco Central se ajustarán a las disposiciones de esta ley que expresamente ésta señale, y a las de sus respectivas leyes orgánicas que versen sobre los asuntos a que se refiere el artículo 1 precedente. También se aplicarán las disposiciones que esta ley expresamente señale a las empresas públicas creadas por ley y a las empresas del Estado y sociedades en que éste tenga participación accionaria superior al 50% o mayoría en el directorio. Los demás órganos del Estado se ajustarán a las disposiciones de sus respectivas leyes orgánicas que versen sobre los asuntos a que se refiere el artículo 1 precedente».

posición permanente del público, a través de sus sitios web,³⁹ diversos antecedentes actualizados, al menos, una vez al mes.

De cara al STDP de los servicios públicos, deben revisarse las letras d) e i). La primera, dispone que lo mantenido en línea será la planta del personal y el personal a contrata y a honorarios, con las correspondientes remuneraciones. La segunda, que cuando dispone transparentar activamente «el diseño, montos asignados y criterio de acceso a los programas de subsidios y otros beneficios que entregue el respectivo órgano, además de las nóminas de beneficiarios de los programas sociales en ejecución», consagra, como excepción legal y para proteger a los beneficiarios, una referencia expresa al artículo 2 de la Ley 19.628.

Esta última opción, la de mantener el resguardo de los datos sensibles o personalísimos de los beneficiarios de los subsidios, coincide con el artículo 10 de la Ley 19.628, que establece como regla general la imposibilidad de su tratamiento. Fue un aporte que en el trabajo parlamentario se haya incluido casi al final de la tramitación legislativa, en una Comisión Mixta de enero del año 2008 y a instancias del senador Larraín y los diputados Cardemil y Eluchans. Junto con incorporarse como antecedentes que debían estar siempre y activamente a disposición del público las nóminas de los beneficiarios de los programas sociales en ejecución, se tuvo la preocupación de reproducir el artículo 2 letra g) de la Ley 19.628 para excluir a sus datos sensibles de dicha publicidad.

El reglamento de la Ley 20.285, a su turno, en el título VI sobre elementos de la transparencia activa y en concreto sobre la letra i), sólo reitera que dentro de los datos o antecedentes de los beneficiarios no se incluirán los datos sensibles, y aclara que por «beneficiario» debe entenderse a la persona natural o jurídica, a la asociación o a la entidad que sean destinatarios directos de los programas sociales.

La regla general en la Ley 19.628 sería la reserva de las remuneraciones de los funcionarios y de los subsidios asignados a los ciudadanos, por tratarse de datos personales sujetos ambos a la obligación de secreto

39. No son muchas las definiciones legales de temas tecnológicos; en este caso, el número 6 del artículo 1 dispone que los sitios electrónicos «también denominados sitios web», son dispositivos tecnológicos que permiten transmitir información por medio de computadores, líneas telefónicas o mediante el empleo de publicaciones digitales.

del artículo 7 y no estar disponibles en fuentes públicas y, los referidos a los beneficiarios, por ser además datos sensibles.

La excepción estaría dada por la Ley 20.285 (lo que a su turno es permitido por el artículo 4 de la Ley 19.628 como un tratamiento-comunicación especial establecido por una ley y sin que se requiera autorización del titular), porque no obstante tratarse de datos personales nominativos procesados en los STDP de los servicios públicos pasan a ser —remuneraciones y subsidios— datos públicos o disponibles en sistemas accesibles al público porque así lo establece expresa y excepcionalmente otro artículo 7 diverso, el de la Ley 20.285.

Incluso más, desde la perspectiva de entender que para la generalidad de la Ley 20.285 existe una opción de política legislativa de garantizar el resguardo de los datos personales, reflejada esta opción sobre todo en los artículos 21 número 2 y número 5 y 33 letra m), estas referencias en el ámbito de la transparencia activa y sin que medie una petición de publicidad o una solicitud de acceso previa y expresa a las remuneraciones o sueldos «de los funcionarios» y a las nóminas «de los ciudadanos beneficiarios de programas sociales» deben ser consideradas excepcionales y de aplicación restrictiva, porque no existen otros datos personales que específicamente deban transparentarse en conformidad al artículo 7.

Por lo mismo, el interés del legislador de la Ley 20.285 por proteger los datos personales y la privacidad, en la búsqueda del equilibrio necesario con el acceso a la información administrativa, queda aún más claro en conformidad con este inciso que en la letra i) del artículo 7, cuando precisa que a propósito de la publicación excepcional de la identidad de los beneficiarios sociales no se incluirán, como contraexcepción, sus datos sensibles de aquellos a que alude la Ley 19.628.

Esta opción legal es coherente además con el artículo 8 de la Constitución de 1980, que aplicado implica que la publicidad de los beneficios sociales adjudicados o asignados no puede extenderse de manera tal que se afecten «a los derechos de esas personas beneficiadas», y por eso se establece la reserva o secreto de sus datos sensibles o personalísimos.

ANÁLISIS DEL ARTÍCULO 21 DE LA LEY DE TRANSPARENCIA Y LAS CAUSALES DE SECRETO O RESERVA ESTABLECIDAS EN LOS NÚMEROS 2 Y 5, EN CONCORDANCIA CON LA LEY 19.628

Luego de velar en el artículo 20 porque los terceros eventualmente afectados por una solicitud de acceso puedan hacer valer sus derechos, y al margen de que esta oposición de un tercero se haya verificado o no (es decir, aun cuando pueda entenderse legalmente que el tercero afectado accedió a la publicidad de la información), el artículo 21 establece — como herramienta para los órganos de la Administración— la tipificación de «las únicas causales de secreto o reserva» en cuya virtud se podrá denegar «total o parcialmente» el acceso a la información, que son las contenidas en los cinco números del artículo. Ergo, el derecho de acceso no es absoluto.

Es un listado taxativo, pero como se ha observado, de causales genéricas o generales que admiten y requieren ser interpretadas, en virtud de las cuales cierto tipo de información y de antecedentes administrativos no pueden ser transparentados o publicados.

La otra opción considerada fue la de establecer causales específicas y detalladas con numerosos ejemplos y referencias de situaciones que podían resultar ambiguas y extender la esfera de secreto,⁴⁰ lo que se descartó, para mantener las genéricas, apoyadas en algunos ejemplos de situaciones precisas, limitadas o específicas donde se concreta la causal genérica y que aportan criterios para lograr que su aplicación sea adecuada. ¿Por qué unas especificaciones y no otras? Soto Velasco (2009: 8) lo atribuye a que el legislador lo hizo no en forma caprichosa, sino que entendiendo que era necesario poner una muy especial atención en las consignadas como ejemplo, en desmedro de otras que podrían ser calificadas como «menos pertinentes».

Es muy acertada la opinión de entender que gran parte de la responsabilidad del Consejo para la Transparencia pasará por dar una adecuada interpretación a estas causales ante su necesidad de acotarlas, y nos sumamos a ella. Lo hacemos desde esta perspectiva: la de entender que limitar o restringir los alcances de la transparencia y el acceso cuando

40. Soto Velasco (2009: 6) menciona como ejemplo una causal que se debatió y se rechazó en el Congreso que aludía a «el acuerdo entre instituciones de Chile y otro país».

estén involucrados datos personales de los ciudadanos mediante la interpretación amplia de las causales referidas a la vida privada o a la privacidad, también implicará la aplicación efectiva de la Ley 20.285 y significará el cumplimiento debido de lo dispuesto por el artículo 33 letra m).

Causales de los números 1, 3 y 4. El número 1 se plantea en el supuesto general de que «la publicidad, comunicación o conocimiento afecten el debido cumplimiento de las funciones del órgano requerido», y «particularmente» (más no exclusivamente) autoriza eximirse de la entrega de los documentos o antecedentes en tres casos:

- si es en desmedro de la prevención, investigación y persecución de un crimen o simple delito o se trata de antecedentes necesarios a defensas jurídicas y judiciales;
- tratándose de «antecedentes o deliberaciones previas a la adopción de una resolución, medida o política» —no siempre, sino caso a caso—, sin perjuicio que los fundamentos de aquéllas sean públicos una vez que sean adoptadas;⁴¹ y,
- tratándose de «requerimientos de carácter genérico, referidos a un elevado número de actos administrativos o sus antecedentes o cuya atención requiera distraer indebidamente a los funcionarios del cumplimiento regular de sus labores habituales»; la evidente amplitud de la causal —señala Soto Velasco (2009: 6)—requeriría, para que no sea invocada frecuente y ligeramente, ser acotada caso a caso mediante la exigencia de pruebas concretas y de criterios objetivos acerca de cómo se verificaría la distracción indebida y de alto costo operativo, antes de optarse por no amparar el derecho a la información y acogerse la causal invocada.⁴²

El número 3 alude al supuesto que «la publicidad, comunicación o conocimiento» afecten la seguridad de la Nación, «particularmente» —y

41. Por cierto, si en el estudio del caso se determina que no se afecta el cumplimiento debido de las funciones del servicio con la publicidad de los antecedentes y deliberaciones previas, estas serán públicas.

42. Un ejemplo posible referido, a tenerse en cuenta al realizarse el test de transparencia, sería el de poner en la balanza los costos de la entrega para el servicio que alega la configuración de la causal de reserva, versus los beneficios invocados por quien solicita la información.

no exclusivamente— si se refiere a la defensa nacional o la mantención del orden público o la seguridad pública. Y el número 4 se refiere al caso de que con «la publicidad, comunicación o conocimiento» se afecte o ponga en riesgo el interés nacional, en especial —pero no exclusivamente, porque son sólo ejemplos—si se refieren a la salud pública, a las relaciones internacionales o a los intereses económicos y comerciales del país. Soto Velasco (2009: 6) menciona, por ejemplo, que también se afectaría el interés nacional si con la petición estuviera comprometida «la política exterior del país».

Causales de los números 2 y 5. Señala el número 2 que es una causal de secreto o reserva, cuando su publicidad, comunicación o conocimiento afecte los derechos de las personas, «particularmente» —a modo de ejemplos los cita la ley— tratándose de su seguridad, de su salud, de la esfera de su vida privada o de sus derechos de carácter comercial o económico.

Como, salvo error u omisión, no encontramos en las actas del debate parlamentario una referencia al respecto, entendemos que debería considerarse que la posible afectación a los derechos «de las personas» incluye tanto a las personas naturales o físicas como a las jurídicas o fictas, porque nada tiene que ver en relación a la tipificación de la causal el que la Ley 19.628 sólo aluda o esté restringida a los antecedentes nominativos de las personas naturales.

Cuando en la causal se alude a «la esfera de vida privada» —lo que por lógica lleva a pensar en un concepto de «lo privado» o de «lo íntimo» opuesto a una también existente y no delimitada «esfera de vida pública»—, o a los «derechos de carácter comercial o económico» de una persona —que es el caso de los llamados datos personales patrimoniales positivos—, normativamente se produce un reenvío no sólo a la Ley 19.628 sino a otras disposiciones.

A la Ley 19.628, porque ella se aboca desde su título a la protección de la vida privada, tanto en cuanto datos o antecedentes personales o nominativos, sensibles o no, de aquellos que la Ley 19.628 sujeta complementariamente a la obligación general de secreto o de reserva para el servicio público en el artículo 7, de aquellos que en los órganos de la Administración no están disponibles en fuentes de acceso público, y de aquellos que son especialmente reservados como los datos sensibles o personalísimos.

Y a otras disposiciones constitucionales, legales y reglamentarias, partiendo por el artículo 19 número 4 de la Constitución, y siguiendo con leyes especiales que establecen su calidad de antecedentes secretos, como es el caso del artículo 35 del Código Tributario.

A su turno, el reglamento de la Ley 20.285 señala, reitera, aclara y detalla en el artículo 7 número 2, que se puede denegar el acceso a la información cuando la publicidad, comunicación o conocimiento afecte los derechos de las personas, especial o particularmente tratándose de su seguridad, su salud, la esfera de su vida privada, sus datos sensibles o sus «derechos de carácter comercial o económico». Agrega que debe entenderse «por tales» a aquellos que el ordenamiento jurídico atribuye a las personas en título de derecho y no de simple interés (o de mera expectativa, podemos agregar).

La reserva que nace de la necesaria protección de la vida privada es un criterio que existió desde la presentación de la moción parlamentaria que originó la ley de acceso y transparencia. Ella aludía a que, dentro de las únicas causales para denegar total o parcialmente el acceso a la información, cabían: i) el que su comunicación o conocimiento afectara la vida privada de una persona individualizada o identificable, incluidos los expedientes médicos o sanitarios;⁴³ y, ii) cuando se pudiesen lesionar intereses económicos o comerciales, sean públicos o privados.

No es casualidad que la causal en comento aluda a que se afecten los derechos de las personas, «particularmente tratándose de su seguridad, su salud, la esfera de su vida privada o derechos de carácter comercial o económico». Esto ratifica la percepción de que la causal puede extenderse o ampliarse en su interpretación y aplicación —lo que potencialmente abre la posibilidad de restringirse el derecho al acceso de la Ley 20.285—, porque pueden invocarse como presuntamente conculcados con la publicidad y por ende sujetos a reserva otros

43. Esta mención era coincidente con lo que estableció en 1999 el artículo 24 de la Ley 19.628, para agregarse los incisos segundo y tercero, nuevos, al artículo 127 del Código Sanitario y disponer que las recetas médicas y análisis o exámenes de laboratorios clínicos y servicios relacionados con la salud son reservados; que sólo podrá revelarse su contenido o darse copia de ellos con el consentimiento expreso del paciente, otorgado por escrito; y que quien divulgue su contenido indebidamente, o infrinja las disposiciones del inciso siguiente, será castigado en la forma y con las sanciones establecidas en el Libro Décimo del mismo Código.

derechos o garantías relacionadas con la seguridad, la salud, la esfera de la vida privada o los derechos de carácter comercial o económico de una persona.

La percepción de que esta causal no está aislada dentro del contexto y la política pública que materializa la Ley 20.285 ha sido compartida en alguna medida por el propio Consejo para la Transparencia, en especial, reconociendo en uno de sus fallos de amparo —en concreto el A53-09—, que el artículo 33 letra m), al obligarlo a velar por la aplicación de la Ley 19.628 en la Administración Pública, complementa este artículo 21 número 2.

En efecto, no sólo refuerza y complementa el numeral 2, sino que hace que la referencia a la «esfera privada» se entienda que alude muy especialmente a los datos personales, nominativos o sensibles que tratan los servicios públicos y que no son parte de la «esfera social o pública» de un ciudadano, y decidir si en concreto un específico dato nominativo cabe dentro de esta esfera privada será responsabilidad del Consejo.

Si la causal genérica en comento que permite la reserva o el secreto es «la posible afectación de los derechos de las personas», una cuestión de hecho que deberá considerarse, interpretarse y acotarse caso a caso por el Consejo es la envergadura que se requiere para considerar que la referida afectación debe generar reserva y la negativa en la entrega de la información solicitada.

Soto Velasco (2009: 7) plantea que ella no puede ser leve o menor y que el riesgo no puede ser lejano o probable, sino que debería considerarse como causal, al ponderarse necesariamente los derechos en juego⁴⁴ y —agreguemos— al realizarse un test de transparencia, sólo cuando la afectación de los bienes jurídicos fuera copulativamente muy probable, directa y grave y así, con este mérito argumentativo «suficientemente sólido», sería válido optarse por preferir el derecho de quien alega la reserva y no amparar el derecho a la información.

El mismo autor citado, pero desde otra perspectiva, plantea que es importante hacer valer y respetar esta causal para no deslegitimar el sistema, porque de divulgarse sin restricciones la información sobre la vida privada de los ciudadanos se perdería «su razón de origen» —que el

44. A saber, el derecho de acceso a la información pública del solicitante y el derecho a la vida privada.

ciudadano pueda controlar al Estado— y pasaría a ser —el sistema—una válvula de acceso a la información privada de los ciudadanos.

Señala el número 5 que es una causal de secreto o reserva, «cuando se trate de documentos, datos o informaciones que una ley de quórum calificado haya declarado reservados o secretos, de acuerdo a las causales señaladas en el artículo 8 de la Constitución Política». Esas causales del artículo 8 se refieren, recordemos, al evento que la publicidad afecte «el debido cumplimiento de las funciones de los órganos del Estado», «los derechos de las personas», «la seguridad de la Nación» o «el interés nacional».

No nos cabe duda en el sentido de considerar dentro de esta causal, cuando se alude a «los derechos de las personas», a la garantía del 19 número 4 sobre el «respeto» —por parte de toda la sociedad— y la «protección» —jurídica— de la vida privada de una persona y su familia y a los derechos que les reconoce la ley 19.628, que es el mecanismo jurídico para cumplir con el mandato de protegerse jurídicamente la garantía constitucional de la privacidad.

ACERCA DE LA INCOMPATIBILIDAD ENTRE EL PRINCIPIO LEGAL DE LA NO NECESIDAD DE EXIGIR EXPRESIÓN DE CAUSA O MOTIVO PARA EL SOLICITANTE Y POSIBLE RECLAMANTE EN EL CONTEXTO DE LA LEY 20.285, CON LOS SUPUESTOS Y PRINCIPIOS ESENCIALES DE LA LEY 19.628

Cuando invocándose las disposiciones de la ley de transparencia y acceso se pida el conocimiento de alguno de aquellos datos personales o nominativos tratados por los STDP de los servicios públicos, tanto el órgano requerido como el Consejo para la Transparencia —conociendo de un reclamo de amparo al acceso—, deberían solicitar la concurrencia de interés legítimo en el solicitante. En caso contrario, los órganos públicos vulnerarían las causales de reserva del artículo 21 número 2 y número 5 pero, muy especialmente, el Consejo para la Transparencia estaría desconociendo el mandato que le impone a su accionar el artículo 33 letra m) y el reenvío que por esta vía se hace a las disposiciones, derechos y principios de la Ley 19.628.

Dicho de otra forma, de no exigir tal interés, motivación o causa y la necesaria legitimación activa que deriva de que el que acciona busque autodeterminar sólo sus propios antecedentes nominativos, sería el pro-

pio Consejo el que no estaría velando por la aplicación de la Ley 19.628, que no admite que cualquier tercero pueda ejercer el *habeas data* del artículo 12 respecto de los datos personales de otro titular.

En principio, las normas legales pertinentes son claras y los dictámenes de amparo del Consejo para la Transparencia —al menos dos de ellos— han sido también claros y perentorios respecto a la no procedencia de exigir expresión de causa o motivo a los solicitantes en el contexto de la Ley 20.285.

El artículo 11 letra g) señala que a la ley la inspira el «principio de la no discriminación», y por ende los órganos de la Administración deberán entregar información a todas las personas que lo soliciten, en igualdad de condiciones, «sin hacer distinciones arbitrarias y sin exigir expresión de causa o motivo para la solicitud». A su turno, el artículo 19 establece que la entrega de copias de los actos y documentos se hará por parte del órgano requerido sin imponer condiciones de uso o restricciones a su empleo, salvo las expresamente estipuladas por la ley.

«Se pide porque se pide, y se debería entregar simplemente porque se pide» sería la formula, pero sabido es que la realidad cotidiana de la gestión del servicio público recurrido no admite esta simplificación. Usando categorías de Soto Velasco (2009: 10), frente a las preguntas acerca de qué se pide, quién lo pide y para qué se pide, en el contexto de la Ley 20.285 y para la ponderación o análisis de las solicitudes de acceso por los servicios públicos —a priori— deberían descartarse de plano la segunda y la tercera interrogante, lo que se percibe como de vital importancia para la aplicación de la ley. Si el criterio fuera distinto, se abriría «una puerta a la discrecionalidad y al análisis de mérito que no corresponde» (Soto Velasco, 2009: 10), porque la única opción que admite la ley para el órgano público es la de invocar algunas de las causales genéricas de reserva o secreto del artículo 21 como posible fundamento de su negativa.

i) El primer pronunciamiento del Consejo, salvo error u omisión, está contenido en la Decisión de Reclamo A8-09 de junio del año 2009 pronunciada en virtud de una supuesta decisión de denegación de acceso de Chilecompra, en concreto, referida a la entrega sistematizada en una base de datos de las licitaciones que se encontraban disponibles en dicho portal en el mes de febrero, las mismas que, en cuanto a su contenido y por mandato de transparencia activa, podían ser consultadas una a una

en el sitio web porque materialmente estaban disponibles y no se negaba el acceso a ellas.

El recurrente declaró que buscaba realizar una actividad económica que consistía en entregar informes y análisis de ellas a sus clientes, práctica que está prohibida por las condiciones y términos de uso de www.chilecompra.cl, por cuanto no sería lícito ejercer tal actividad económica a partir de bienes —la data— que no son de propiedad de los usuarios de la plataforma.⁴⁵

En concreto, más que sobre el derecho de acceso del recurrente, la real discrepancia entre el recurrente de amparo y el servicio recurrido era acerca de las condiciones establecidas para el uso que debía darse a información ya disponible en línea en el sitio web del órgano.

El Consejo estimó (considerando sexto) que dichas condiciones no eran válidas, porque el artículo 19 dispone expresamente que la entrega de copias de los actos y documentos se hará por parte del órgano requerido —por regla general— sin imponer condiciones de uso o restricciones a su empleo «que no estén establecidas expresamente por una ley», y las condiciones o los términos de uso del sitio www.chilecompra.cl no lo están de modo alguno, lo que era aplicable a toda la información pública que se solicitara a través del procedimiento de acceso a la información de los artículos 12 y siguientes

ii) El pronunciamiento anterior fue ratificado en julio del 2009 en la Decisión de Amparo A54-09, formulada en consideración a un reclamo de amparo interpuesto en contra del Servicio de Impuestos Internos.

En el considerando octavo, al hacerse cargo de una de las alegaciones del SII en cuanto a que el único interés del recurrente al solicitar la información era lucrar con ella, y para aplicar literalmente y sin consideraciones la Ley 20.285, se cita la Decisión de Reclamo A8-09 de junio del año 2009 pronunciada en contra de Chilecompras, i) para recordarla específicamente en la parte que se cita que el artículo 19 dispone que la entrega de copias de los actos y documentos se hará por parte del órgano requerido por regla general sin imponer condiciones de uso o restriccio-

45. Concretamente, lo prohibido es usar la plataforma para consultar información de bienes o servicios y hacer cotizaciones, ni reproducir o comercializar con fines de lucro dicha información y las funcionalidades del sitio web; sería el caso, por ejemplo, si se establecieran vínculos sin autorización a sitios comerciales o de ofertas de consultoría.

nes a su empleo que no estén establecidas expresamente por una ley, y, ii) para conciliarla con el principio del artículo 11 letra g), que establece que los órganos deben entregar información a todas las personas que lo pidan en igualdad de condiciones, sin hacer distinciones arbitrarias y sin exigir expresión de causa o motivo para la solicitud.

La finalidad del recurrente del amparo del artículo 24 era obtener una mera finalidad de lucro, y no fiscalizar la probidad de las actuaciones del Servicio de Impuestos Internos. ¿Cabe entender que los servicios públicos deban destinar sus recursos para permitir la generación de negocios sin fines de servicio público alguno? Creemos que no, que si las peticiones se tornan masivas o múltiples se entrabará la gestión del órgano del Estado, y que entenderlo como lo ha hecho el Consejo, sin límites, sin matices y en forma extrema, literal y absoluta, es contrario en definitiva a los fundamentos y a la política pública subyacente en la Constitución Política y en la Ley 20.285.

No obstante, lo anteriormente dicho en cuanto a la regla general de la no exigencia de expresión de motivo o causa para el ejercicio del acceso a la información administrativa, es una regla general que, si queremos hacerla coexistir con la normativa chilena de protección de datos personales, debe admitir excepciones.

Atendido que el artículo 33 letra m) de la ley de acceso y transparencia establece la obligación de que el Consejo vele por el cumplimiento adecuado de la Ley 19.628, una de las consideraciones esenciales a ser tenidas en vista al resolver las solicitudes de amparo es que la segunda normativa exige que el acceso a los datos personales sólo pueda ser solicitado única y exclusivamente por el titular individualizado por los datos personales tratados computacionalmente, que es lo que le concede la calidad de legitimado activo poseedor de un interés legítimo, esto es, el de autodeterminar y controlar —en conformidad al artículo 12 de la ley 19.628— únicamente el uso de sus propios antecedentes tratados por los servicios públicos, y no el de poder conocer los datos nominativos de terceros.

De lo anterior, se concluye necesariamente, en primer lugar, que no cabe aplicar en el ámbito de la protección de datos personales de la Ley 19.628 el criterio de que cualquier persona sin señalar interés legítimo puede solicitar antecedentes nominativos de otra. Y, en segundo lugar, en el contexto de transparencia y acceso de la Ley 20.285, que si lo soli-

citado por el recurrente de amparo son datos personales o nominativos que no lo individualizan ni son atributos de su personalidad, el Consejo debiera resolver la negativa del acceso y de la entrega de los antecedentes, por cuanto la misma Ley 19.628 que está llamado a velar para que se aplique en virtud del artículo 33 letra m) debe percibirse como una excepción a la regla general de la no exigencia de interés legítimo o, concretamente, de la no expresión de causa o motivo.

Si frente a una solicitud de acceso relacionada con datos nominativos el velar por la privacidad de los ciudadanos, tanto en cuanto datos personales tratados por los servicios públicos, también es una competencia legal del Consejo para la Transparencia, creemos que cuando el Consejo constate que la transparencia se topa con la privacidad debe optarse por la privacidad, porque en caso contrario se estaría incumpliendo la obligación legal del artículo 33 letra m). Decisiones de amparo como la número A117-09, donde se negó el acceso a datos personales sensibles tratados por un municipio, ratifican este planteamiento, más allá de que lo dictaminado haya sido atendido la concurrencia clara y fundada de una de las causales de reserva del artículo 21 de la Ley 20.285.

Sirve como ejemplo nuevamente el caso referido más arriba. Ante una solicitud de una empresa distribuidora de información de acceder en forma asociada a los datos personales RUT y roles de avalúo de un ciudadano, cada uno de los propietarios de bienes raíces poseerá una «causa suficiente» para oponerse a la solicitud de acceso con fines comerciales (porque ahora se debe calificar si es legítimo o no el interés de la solicitud, al relacionarse con las garantías de la Ley 19.628). Y por no existir un interés legítimo y por no tratarse de una solicitud realizada en forma individual, aislada o no masiva sólo por el titular de los datos personales, único legitimado por el artículo 12 de la Ley 19.628, la solicitud debiera rechazarse.

i) Si para la Ley 19.628 y su artículo 4 se requiere consentimiento del titular de los datos tratados —lo que en alguna medida guarda relación con la obligación de notificar a terceros del artículo 20 de la ley de acceso y transparencia, porque este «traslado» precisamente permite que la norma se concrete y el titular autodetermine el uso de sus antecedentes—; y, ii) si el artículo 12 sólo legitima al titular de los datos nominativos para ejercer el *habeas data* y controlar sus datos personales —por este sólo hecho, causa o motivo de ser el titular—, esto no guarda

relación con el «principio de la no discriminación» de la ley de acceso y transparencia, de acuerdo al cual los servicios públicos deberán entregar información a cualquier persona que lo solicite y sin exigir expresión de causa o motivo para la solicitud.⁴⁶

Tanto la Ley 19.628 como la 20.285 reconocen la existencia de los datos sensibles o de los personales especialmente protegidos, lo que nos ha llevado a sostener que la referencia a ellos en la ley de acceso y transparencia no es sino una nota que refleja la clara política pública de resguardo y preferencia de los datos personales que subyace, lo que no es un detalle menor. Ambas normas exigen un actuar administrativo diligente. La Ley 20.285 lo hace de partida cuando en la letra j) del artículo 11 consagra el principio de la responsabilidad, conforme al cual el incumplimiento de las obligaciones que impone a los órganos de la Administración origina responsabilidades y da lugar a las sanciones; en la letra f) al enunciar el «principio de facilitación», conforme al cual los mecanismos y procedimientos para el acceso a la información de los órganos de la Administración deben facilitar el ejercicio del derecho y excluir exigencias o requisitos que puedan obstruirlo o impedirlo; y en la letra h) que consagra el «principio de la oportunidad», el que implica que los servicios deben proporcionar respuesta a las solicitudes de información dentro de los plazos legales, con la máxima celeridad posible y evitando todo tipo de trámites dilatorios.

De la Ley 20.285, por último, nunca podrían tener cabida en la aplicación de la Ley 19.628 los siguientes otros principios: i) el «principio de la libertad de información», de acuerdo al cual toda persona goza del derecho a acceder a la información que obre en poder de los servicios públicos y con las solas excepciones o limitaciones establecidas por leyes de quórum calificado; y, ii) el «principio de máxima divulgación», en cuya virtud los órganos de la Administración del Estado deben proporcionar información en los términos más amplios posibles, excluyendo sólo aquello que esté sujeto a las excepciones constitucionales o legales.

46. En sede de protección de datos en cambio, los servicios públicos sólo deben atender las peticiones de *habeas data* o derecho de acceso para controlar y autodeterminar los datos personales cuando sean realizadas por los propios titulares individualizados y teniendo como motivo o causa suficiente el sólo hecho de serlo, pero sin que puedan entorpecer la gestión de la Administración del Estado.

Un ejemplo concreto puede servir para relevar cómo debiera ser rechazada una solicitud de acceso, a partir de la importancia que la institucionalidad de la protección de datos personales le asigna al hecho de que los servicios públicos sólo pueden tratar-comunicar los datos personales cuando ello sea de su competencia de Derecho Público, y en segundo lugar, a que el tratamiento que realicen sólo obedezca a la finalidad de cumplir con los fines promocionales y asistenciales que le son propios.

Sería el caso en que una agencia de viajes le solicitara al Servicio de Registro Civil una base de datos —masiva, sistematizada y fidelizada, sin «ruidos» ni «silencios»— con los nombres, RUT y domicilios de las personas que se hubieran casado dentro de los seis meses anteriores a la petición, a efectos de ofrecerles planes turísticos de luna de miel y/o de recién casados.

En el contexto de la ley de acceso y transparencia a esta fecha el Consejo es probable que resolvería el reclamo señalando que sin importar quien lo pide y la finalidad con que se hace, el Registro Civil debiera entregar la información porque ella está contenida en las actas y bases de datos del servicio y porque por ley es de su competencia exclusiva la entrega de la información mediante certificados de matrimonio que se comercializan, donde ambos —actas y certificados— son documentos públicos.

Pero no es de competencia del Servicio de Registro Civil el informar quiénes han sido los nacionales que contrajeron matrimonio específicamente los seis meses anteriores a la solicitud, individualizándolos en conformidad a sus nombres, números de RUT y domicilios. Nosotros esperaríamos que al tratarse de datos personales los calificara de personales y secretos para un tercero solicitante diverso del titular, que aparece pidiéndolos en forma masiva, sistematizada, fidelizada y no unitaria, sin pagar el costo de los certificados y sólo cancelando los costos directos de generación o reproducción y de soporte a que alude el artículo 18.

Si este mismo Consejo asume la obligación del artículo 33 letra m) y aplica los principios de la protección de datos personales, debiera considerar: i) que no existe competencia alguna asignada al Registro Civil para ser proveedor de datos personales en forma masiva; ii) que la entrega solicitada no persigue fines de servicio público sino sólo comerciales o de lucro; iii) que la competencia legal que el órgano posee para tratar los datos sobre estado civil de los chilenos sólo llega hasta la eventual certificación caso a caso o uno a uno cuando se le solicita la certificación

de los antecedentes de sólo una persona o un RUT determinado; iv) que generar esta información distrae indebidamente a los funcionarios del cumplimiento de sus labores habituales; y v) que si bien es cierto los contrayentes y/o cónyuges no pueden oponerse a que se pida un certificado asociado a un sólo RUT de ellos cuando éste se individualiza, al ser notificados para oponerse en conformidad al artículo 20 se hiciera valer el que se está pidiendo información que el Registro Civil trata con una finalidad específica para fines distintos y de mero lucro.

ACERCA DE LA ILEGALIDAD DE UNA «INSTRUCCIÓN» EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES EMANADA DEL CONSEJO

El año 2011 fue convocada por el Consejo para la Transparencia una consulta pública, a efectos de recibir comentarios sobre una propuesta de «recomendación» en materia de protección de datos personales al interior de los servicios públicos.

Si bien es cierto el documento aprobado en definitiva es un buen resumen dogmático de la Ley 19.628 de Chile —a lo cual contribuimos con un Informe en Derecho encargado por el Consejo al efecto—, esa competencia que le asignó el artículo 33 letra m) de la Ley 20.285 y que hemos referido más arriba, consistente en «velar por la aplicación de la Ley 19.628 en los servicios públicos», no puede leerse sino como un complemento de las otras normas de la ley de acceso a la información y transparencia.⁴⁷ No es, de modo alguno, un mandato abierto para «instruir» ahora bajo la denominación de «recomendación», reglamentar y establecer nuevos requisitos no contemplados en el texto de la Ley 19.628, crear procedimientos de reclamo de *habeas data* ilegales, y autoasignarse competencia para conocer alternativamente de los recursos del artículo 12 de la Ley 19.628, lo que nunca estuvo ni en el espíritu ni en el debate del legislador de la Ley 20.285.

47. Lo dicho, lo sostenemos pensando por ejemplo: i) en la obligación de velar por el resguardo y/o la confidencialidad de los datos personales de los ciudadanos, de sus antecedentes sociales y personales sensibles en sede de transparencia activa; y ii) ante la obligación de ponderar adecuadamente cuando conozca de un recurso de amparo al derecho de acceso el alcance de las causales de reserva o secreto establecidas en el artículo 21 de la Ley 20.285, en cuanto se relacionen con los derechos de las personas, tratándose de su seguridad, su salud y de la esfera de su vida privada.

Cuando la Ley 20.285 se refiere a las facultades de dictar instrucciones y recomendaciones declara explícitamente la dimensión en la que se puede mover el Consejo y en ella no queda comprendida la protección de datos. De ahí en adelante, y sin ese piso legal, lo que viene es ilegal. Lo establecido en el artículo 33 letra m) es una competencia limitada. Esta facultad no se puede extender al punto de considerar que estamos frente a la nueva Autoridad o Agencia de Protección de Datos chilena, y de creer que el Consejo posee competencia procesal y administrativa para conocer de reclamos en que se invoque la no aplicación o respeto de la Ley 19.628 por los servicios públicos.

Falta en esta recomendación alguna referencia a los artículos 7 y 21 número 2 de la Ley 20.285. Es decir, para empezar diciéndole a los servicios públicos que no transparenten activamente más datos personales que aquellos que excepcionalmente se permite (remuneraciones y subsidios asignados); y para recalcarles que es causal de secreto o reserva y de no entrega cuando se soliciten documentos sobre su gestión que contengan datos sobre la vida privada de los ciudadanos o, derechamente, únicamente cuando se les pidan estos datos en forma aislada. La omisión se explica porque el Consejo no es una autoridad de protección de datos y han demostrado que no llevan en su ADN la importancia de velar por la privacidad de los chilenos.

La relación entre la protección de datos personales o el *habeas data* y el derecho de acceso a la información de la gestión del Estado no son, de modo alguno, «las dos caras de la misma moneda». De hecho, la cara del *habeas data* de la Ley 19.628 es esencial en un mundo no relacionado con la gestión de los servicios públicos, es decir, en el sector privado y para que las personas controlen sólo el uso de sus datos personales. Y a propósito de la gestión de los órganos del Estado, con el norte de transparentarla para evitar faltas a la probidad y corrupción que es la razón de ser de la Ley 20.285, tanto el artículo 8 de la Constitución de 1980 como los artículos 7 y 21 de la ley de acceso son claros en el sentido de la necesidad de restringir y resguardar la reserva y confidencialidad de los datos personales. Lo que en verdad ocurre que son monedas o billetes de diverso cuño y de distinto valor que sirven para pagar conflictos jurídicos diversos.

Y tampoco la protección de datos personales, que nace en la década de los setenta, es una especie del moderno género de acceso a la infor-

mación del Estado; la primera es una restricción del segundo, y no debe perderse de vista esta idea. Como tampoco debe olvidarse que el *habeas data* del artículo 12 de la Ley 19.628 no necesita para ser ejercido de un ámbito de posible falta de transparencia, posible falta de probidad o posible corrupción, que es el único donde puede operar con competencia el Consejo para la Transparencia.

No es menor que el Consejo olvide que tanto las competencias como las interpretaciones de Derecho Público sólo deben hacerse por ley o por órganos (como el Tribunal Constitucional) con competencia para hacerlo, que no es el caso del Consejo. Ahora, al «instruir» bajo la carátula formal de «recomendar» en los numerales 5.1 inciso cuarto y 5.12 inciso tercero pretende ilegalmente autoasignarse la competencia de conocer directa y alternativamente de los *habeas data* contemplados en el artículo 12 de la Ley 19.628; Dicen que si un titular de datos personales no quiere seguir el camino judicial para ejercer el *habeas data* del artículo 12, puede optar por hacerlo ante el Consejo para la Transparencia y esto —asignarse competencias de Derecho Público— es ilegal.

Ya antes el Consejo había interpretado que tácitamente cuando se pedía un documento con datos personales y aunque el recurrente en virtud del amparo del artículo 24 de la Ley 20.285 no lo supiera ni tuviera la intención de hacerlo, se estaba ejerciendo tácitamente una especie de *habeas data* «impropio». No se debe olvidar que se trata de un derecho personalísimo que sólo puede ejercerse expresamente por los propios titulares de los datos personales y en la forma que establece la Ley 19.628; pero ahora, en la «recomendación-instructiva» propuesta profundiza esta interpretación ilegal carente de todo fundamento jurídico y lo declara formalmente.

En paralelo, las decisiones del Consejo al conocer de las acciones de amparo reguladas por el artículo 24 de la ley de acceso y transparencia que ya hemos cuestionado, han reflejado la falta de sensibilidad de un órgano que nace para transparentar con la necesidad de proteger la privacidad, tanto en cuanto datos personales procesados computacionalmente. A la irresponsabilidad de ordenar la entrega a cualquiera y sin tener que declararse motivo que justifique la petición de los datos de los discapacitados registrados en el Servel y de las calificaciones de miles de funcionarios públicos, se suma una decisión que ordenaba que se entregara a un ciudadano que sólo perseguía fines de lucro el detalle

de todas las operaciones de compraventa de bienes raíces celebradas durante varios años, lo que vulneraba normas expresas de secreto tributario y el artículo 19 número 4 de la Constitución; pero el Consejo, no lo entendió así.

Quizás por estos criterios reiterados y equivocados, un fallo de la Corte de Apelaciones de Santiago de enero del 2011 ha llamado al orden al Consejo para la Transparencia.⁴⁸ La claridad de sus considerandos es de antología. Conociendo de un reclamo contra la decisión del Consejo que obligaba a entregar a una persona que no invocaba motivos legítimos y que sólo tenía fines de lucro los detalles de las operaciones de compraventa de bienes raíces durante varios años, señaló: i) en el considerando décimo tercero, que no se estaba pidiendo información alguna que hubiera sido ocultada, silenciada o no transparentada, sino que ella era de público acceso pero disponible en el Conservador de Bienes Raíces; ii) en el décimo cuarto, que el servicio público que no entregó los datos no infringió los principios rectores de la Ley 20.285 ni el espíritu del Constituyente, porque nada ocultó ni nada omitió; iii) en el décimo quinto, que el reclamante de amparo al cual el Consejo le dio la razón en desmedro de la protección de datos personales no estaba con su petición contribuyendo a fortalecer la transparencia de la función pública ni a la reducción de los posibles ámbitos de corrupción y que no estaba ejerciendo un control democrático de la gestión estatal; y iv) en el décimo sexto, que las solicitudes de los peticionarios si debían contener intereses legítimos, ya que en caso contrario (aplicándose el criterio reiterado del Consejo) se caía en un caso de abuso del derecho.

Siempre a propósito de las malas interpretaciones del Consejo, están haciendo una muy mala aplicación de los artículos 4, 5 y 10 de la Ley 20.285. O bien, una aplicación abiertamente contraria a los principios de la Ley 19.628 y a la garantía del artículo 19 número 4.

Es esencial definir hasta dónde llega o cuál es el alcance jurídico de la referencia a «todo otro tipo de información que obre en poder de la Administración o que sea elaborada con fondos públicos», de los artículos 5 y 10 de la Ley 20.285, para entender —o no (que es nuestro parecer)— que los datos personales *per se* no se pueden considerar incluidos junto a los

48. Sentencia de la I. Corte de Apelaciones de Santiago, causa rol 6143-2010, de 28 de enero de 2011.

actos, contratos, resoluciones, procedimientos y documentos que deben ser públicos al estar en poder de los servicios públicos y accesibles para cualquier persona que los solicite, sin expresar causa o motivo legítimo.

No existe debate alguno en las actas parlamentarias que haya concluido en la opción de la inclusión; la institucionalidad de la protección de datos personales se opone a la inclusión; y no respetar lo establecido en los artículos 8 de la Constitución y 21 número 2 de la Ley 20.285 para entender que en esta referencia amplia sólo se subsumen antecedentes que den cuenta de una gestión del Estado corrupta, poco transparente o poco proba, y no datos personales o nominativos, ha llevado a que algunas decisiones del Consejo configuren casos de «abuso del derecho».

Si bien a nivel del principios en el artículo 11 letra c) se consagra el principio de apertura o transparencia, conforme al cual «toda la información en poder de los órganos de la Administración del Estado» se presume pública, salvo leyes de quórum calificado que establezcan lo contrario, esta presunción de publicidad no puede extenderse, con fundamento jurídico serio, a los datos personales o nominativos.

Adicionalmente, si retomamos el inciso segundo del artículo 5 de la Ley 20.285 cuando establece que «es pública toda otra información que obre en poder de los órganos de la Administración», y tenemos presente la definición esencial del contenido del principio de transparencia del inciso segundo del artículo 4, debe concluirse que sólo será pública la información administrativa que por su naturaleza sea factible de «facilitarse su acceso» a cualquier persona, sin que se le exija a ella expresión de causa o motivo al solicitar conocerla. Pues bien, esta condición no concurre respecto de los datos personales o nominativos de los administrados que sean tratados por los servicios públicos,⁴⁹ porque ellos y en conformidad al artículo 12 de la Ley 19.628 sólo son accesibles para su propio titular, y porque a su respecto existe —para los responsables del tratamiento en el órgano administrativo— la obligación general de secreto del artículo 7 de la misma ley.

49. La excepción estará dada por los datos personales que provengan de fuentes públicas a cuyo respecto el servicio público tenga competencia para darlos a conocer, o cuando estemos frente a datos personales contenidos en documentos como certificados o resoluciones que, también por ley, sea de la competencia exclusiva del servicio público el emitirlos (Registro Civil, TGR, Aduana, SII, etcétera).

Sigue pendiente y suena fuerte el afán del Consejo para la Transparencia por desnaturalizarse, y transformarse en la nueva autoridad chilena de protección de datos personales. Es decir, dejar de transparentar documentos del Estado para velar por la privacidad y confidencialidad de los datos personales de los chilenos —ya no tan sólo en el contexto de la gestión de los servicios públicos—, sin tener la idoneidad ni la preparación necesaria.

Esperan tener el presupuesto y el respaldo para hacerlo; siguen apostando a que se tramite un Boletín modificatorio de la Ley 19.628, que presentado sin un debate previo y serio por el Ministerio Secretaría General de la Presidencia en el año 2009 se preparó para cumplir con los requisitos de incorporación a la OECD; afirman seguir un modelo inglés, sin decir que bajo un mismo paraguas formal existen dos entes diversos y que ha sido deficitario para la protección de datos; minimizan la opción mayoritaria e idónea de que existan dos entes diferenciados, uno para la protección de datos y otro para el acceso a la información de la gestión del Estado, poniendo al mismo nivel las opciones deficitarias de Inglaterra y México con las de Canadá, Francia, España o Argentina; no avanzan en las propuestas de mejoras de fondo a la Ley 19.628, y se contentan, sin crítica alguna, con decir que en 1999 no podía hacerse otra cosa porque sólo la evolución del tratamiento de datos personales la hizo tan deficitaria; y realizan lobby parlamentario y ante el Ejecutivo al efecto. Pero la solución que esperan los chilenos en materia de institucionalidad de protección de datos no pasa por asignar competencias a entes no idóneos.

Lamentablemente, siguen sin hacerse cargo de los argumentos en contrario de un informe neutral de una Escuela de Ingeniería que ellos mismos encargaron.⁵⁰ En las páginas 110 y 111 del estudio, de forma clara y directa, se consigna que no es idóneo tener en una misma institución las funciones de protección de datos y de acceso a la información; que la experiencia internacional recogida demuestra que en su gran mayoría los temas los abordan agencias diversas; que es crítico el desconocer que se trata de «negocios» muy distintos, considerando los principios involucrados, las funciones que deben desarrollarse (transparentar una

50. Véase <http://www.consejotransparencia.cl/consejo/site/artic/20100614/asocfile/20100614185659/informe_pdatos.pdf>.

y resguardar la confidencialidad y privacidad de los datos personales), los sectores donde operan (no hay acceso en el sector privado) y que los conflictos de intereses se presentan también en ámbitos muy diversos.

REFERENCIAS

JIJENA LEIVA, Renato (1992). *Chile, la protección penal de la intimidad y el delito informático*. Santiago: Jurídica.

—. (2001). «La ley chilena de protección de datos personales: una visión crítica desde el punto de vista de los intereses protegidos». En *Estudios sobre la Ley 19.628 sobre protección de datos de carácter personal*. Cuadernos de Extensión Jurídica, 5, Facultad de Derecho Universidad de Los Andes.

MINISTERIO SECRETARÍA GENERAL DE LA PRESIDENCIA (2004). Informe de agosto del año 2004, elaborado por la Secretaría Técnica de un Comité multidisciplinario de análisis del tratamiento de datos personales en los sitios Web del Estado.

SOTO VELASCO, Sebastián (2009). «Ley de Transparencia: desafíos en su aplicación». *Revista Temas de la Agenda Pública*, 4 (30).

SOBRE EL AUTOR

RENATO JIJENA LEIVA es abogado. Licenciado en Ciencias Jurídicas por la Pontificia Universidad Católica de Valparaíso, diplomado en Derecho Informático por la Universidad de Zaragoza, España y magíster en Gobierno Electrónico por la Universidad Tecnológica Metropolitana, Chile. Profesor de Derecho Informático en la Escuela de Derecho de la Pontificia Universidad Católica de Valparaíso. Su correo electrónico es <renato@jjjena.cl>.

Este trabajo fue recibido el 23 de agosto de 2013 y aprobado el 30 de diciembre de 2013.